25TH ANNIVERSARY
MCLE SPECTACULAR!
Friday, November 22, 2019

The CCCBA Business Law Section proudly presents...

#5 Wild West of Law Firm Cybersecurity & Privacy: The What, Why, How & Ethics of Protecting Client Data

Joshua Bevitz - Newmeyer & Dillon
Darryl Holcombe - CCC District Attorney's Office - Internet Crimes
Emma Raimi-Zlatic - Clio
Ashley L Shively - Holland and Knight

AGENDA

A. Introductions

B. The California Consumer Privacy Act ("CCPA") and how it applies to the legal profession.

Disclosure obligations | Consumer rights | Enforcement
Duty to reasonably secure information | New California Ballot Initiative

C. A Law Firm's Ethical Duties to Protect Client Data

D. Data Breach Notification Requirements for Law Firms

E. Utilizing Law Firm Technology to Protect Client Data

How Cloud Technology Protects Law Firms & Clients
Stats on Cybersecurity Preparedness
Internal Best Practices for Cybersecurity
Due Diligence for Evaluating Legal Technology

F. Law Enforcement's Response to Data Breaches

G. Protection Efforts from a Law Enforcement Perspective

H. Questions

NEWMEYER DILLION

Joshua Bevitz

Partner

joshua.bevitz@ndlf.com

Walnut Creek, CA: 925-988-3226

Joshua Bevitz is a legal strategy pioneer who develops creative litigation solutions to address the individual needs of each of his clients. He concentrates his legal practice on real estate, construction, business litigation, and cybersecurity. As partner in the Walnut Creek office of Newmeyer Dillion, Joshua advises developers, builders, contractors, and other businesses on a variety of real estate, construction, insurance, and cybersecurity related claims. He has experience litigating cases in both state and federal courts, resolving cases through alternative dispute resolution, and in enforcing judgments.

Joshua also worked for the U.S. Department of Justice, Criminal Division, Office of International Affairs in Washington D.C. While in law school, Joshua was an Executive Editor of the Hastings Law Journal, which published his law school note, Flawed Foreign Policy: Hypocritical U.S. Attitudes Toward International Criminal Forums, 53 Hastings L.J. 931 (2002). Joshua also earned credits at Trinity College in Dublin, Ireland and Charles University in Prague, Czech Republic and honors in his Moot Court and Appellate Advocacy courses.

Services

- Business & Commercial Litigation
- Construction Defect Litigation
- Risk Avoidance, Transfer & Management
- Privacy & Data Security
- Real Estate Litigation

Education

- University of California, Hastings College of Law *(J.D., 2002)*
  - International Law Concentration

NEWMEYER DILLION

- Washington University *(B.A., 1997)*
  - English Literature
  - Minor in Writing
- Washington University *(B.S., 1997)*
  - Business, Law, and Economics Concentration

Emma Raimi-Zlatic is Affinity Program Manager at Clio, the world's leading cloud-based technology platform offering legal practice management, client intake and CRM software for legal professionals. Having had nearly a decade of unique experience in both legal and tech herself, Emma understands the needs of lawyers and law firms and is passionate about helping the legal industry bridge the gap in technology. She regularly speaks on tech-related topics at conferences and events, including on subjects related to cloud computing, data privacy & security, law firm marketing, client intake and law firm automation.

She has a JD from the University of Houston Law Center, and has previously worked in the legal field for an international law firm and government agency, as well as for non-law related tech startups in Silicon Valley. In addition, she also founded an attorney recruiting company prior to joining Clio. As a founder, Emma knows first-hand the importance that technology and security play in growing a business, and often uses her experience as a reference when advising others. She can be reached at emma.raimi@clio.com, and is based in Los Angeles, CA.

Ashley L. Shively

Partner

San Francisco
415.743.6906
Ashley.Shively@hklaw.com

Ashley L. Shively is a class action litigator and privacy attorney in Holland & Knight's San Francisco office. She focuses her litigation practice on the defense of financial institutions and businesses in consumer class and individual actions, including fair lending, data breach, privacy, credit reporting, debt collection, false advertising and unfair business practices. Ms. Shively has extensive experience litigating class actions under the Truth in Lending Act (TILA), Telephone Consumer Protection Act (TCPA), California's Invasion of Privacy Act (CIPA), and Illinois Biometric Information Privacy Act (BIPA).

Ms. Shively also handles complex litigation matters, from mass tort and federal multidistrict litigation to commercial contract disputes. She represents public agencies and private businesses affected by litigation brought under the California Public Records Act, and clients in matters involving the FCC and other regulatory agencies.

Ms. Shively counsels FinTech and financial services companies on consumer protection issues with respect to product development, regulatory compliance, and state and federal enforcement. She has substantial experience advising companies on privacy issues and legislative developments as well as compliance with state, federal and international privacy laws and regulations. At present, she is particularly focused on the California Consumer Privacy Act (CCPA) and similar legislation that has been introduced in other states.

Ms. Shively previously worked in the civil division of the Superior Court of California of the County of Alameda. She also externed during law school for the Honorable Frank C. Damrell in the U.S. District Court for the Eastern District of California and the Honorable Robert L. Dondero in the Superior Court of California of the County of San Francisco.

Education

- University of California Davis School of Law, J.D.
- The Johns Hopkins University, M.A., Government
- The Johns Hopkins University, B.A.

Darryl Holcomb currently works for the Contra Costa County District Attorney's Office in Martinez. He handles investigations such as Internet Crimes Against Children using peer to peer investigative software, to locate individuals downloading and sharing child pornography. He is currently the team leader for the Contra Costa County affiliate ICAC task force.

He is a Task Force Officer with the US Secret Service Electronic Crimes Task Force and currently investigates cybercrime, cyberstalking and child exploitation cases.

In 2016, he attended the National Computer Forensics Institute's five week BCERT course in Hoover, Alabama. He conducts digital forensic investigations with proficiency using Encase, IEF, FTK, Cellebrite, Blackbag and other forensic tools.

He serves as the Cal ECPA coordinator for the County and develops training courses for Officers in the County, reviews warrants and provides feedback to prosecutors on ECPA issues.

EXPERIENCE

Contra Costa County District Attorney Nov 2011 – Present
Senior Inspector (Criminal Investigator)

-
- **Concord Police Department**
  Police Officer - Aug 2001 – Nov 2011
  Corporal - Apr 2008 – Jul 2011
  Detective Jul 2004 – Jul 2007
  -Investigated a wide range of fraud related crimes, including identity theft, computer fraud, bank fraud and embezzlement.
  -Prepared and served legal documents such as search warrants, arrest warrants and seizure orders.
  -Coordinated investigations with other local, state and federal agencies.
  -Prepared cases for filing with local, state and federal prosecutors

HONORS & AWARDS

- **Excellence in the Pursuit of Justice** United States Attorney, NDCA **-** Nov 2018
- **Medal of Merit** Oakley Police Department **-** Nov 2018
- **Top forensic examiner** United States Secret Service **-** March 2018
  FBI Directors Award- Internet Crimes Against Children - May 2017
  Internet Crimes Against Children
- **Senior Inspector of the Year** CCC District Attorney's Office **-** Mar 2016

Holland & Knight

ALERT

California Consumer Privacy Act Amendments Head to Gov. Newsom's Desk

September 20, 2019

Ashley L. Shively

HIGHLIGHTS:

- The California State Legislature has passed five bills to amend the state's landmark privacy legislation, the California Consumer Privacy Act (CCPA). Gov. Gavin Newsom has until Oct. 13, 2019, to sign or veto the legislation, and the order in which he enacts bills will determine whether some overlapping provisions of the bills are enacted or not.
- Further complicating companies' efforts to operationalize the CCPA is the fact that regulations are still forthcoming. The state attorney general is expected to release draft regulations sometime this fall.
- In the absence of comprehensive federal privacy legislation, California has moved forward on its own, and the CCPA will come into effect on Jan. 1, 2020, alongside a number of other generally pro-consumer privacy laws.

Five bills to amend California's landmark privacy legislation, the California Consumer Privacy Act (CCPA), passed the California State Legislature last week and now head to Gov. Gavin Newsom's desk. (See Holland & Knight's previous alert, "California Consumer Privacy Act Update: Assembly Approves 12 Amendments," June 6, 2019.)

New Exemptions to Portions of the Act

Employees Are Out of Scope (Partially and at Least for Now). Introduced to address industry concern that employees would be covered by CCPA's broad definitions, **AB 25** would exempt from most provisions of the Act personal information collected by a business from "a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business" when the individual is acting in such capacity.

The bill includes two notable exemptions:

1. A business would still be required to inform applicants, employees, contractors, etc. as to the categories of personal information to be collected by the business in the course of the individual acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of or contractor of that business
2. Applicants, employees, contractors, etc. would still be entitled to bring a private right of action for a data breach under Section 1798.150

Unless the legislature acts next year, the exemption would sunset on Jan. 1, 2021, and applicants, employees, contractors, etc. would be within the scope of the Act for all purposes, meaning such individuals could then make access and deletion requests to prospective, current and former employers.

Some Vehicle Information Exempted. **AB 1146** would exempt vehicle information — VIN, make, model, year, odometer reading, and name and contact information of the registered owner — retained or shared between a new motor vehicle dealer and the vehicle's manufacturer, if such information is shared for the purpose of effectuating repairs covered by a warranty or recall, and provided that such information is not used, shared or sold for any other purpose.

Changes to Consumer Rights Request Process

Two bills would make changes to the consumer rights request process.

Online Businesses Need Not Provide Telephone Number for Rights Requests. **AB 1564** would reduce the burden on online-only businesses, and permit such businesses to provide only an email address for consumers to submit rights requests.

Reasonable Authentication Measures Acceptable. To address concern about potentially fraudulent or malicious consumer rights requests, **AB 25** would authorize a business to require authentication of the consumer that is reasonable in light of the nature of the personal information requested. The bill would also authorize a business to require a consumer/account holder to submit a verifiable consumer request through an account that the consumer maintains with the business. A business would still be prohibited from requiring a consumer to create an account in order to submit a request.

Businesses Need Not Delete Warranty-Related Information. **AB 1146** would add a new circumstance where a business need not delete personal information: to fulfill the terms of a written warranty or product recall conducted in accordance with federal law.

Clarification of Non-Discrimination Provision. Current law provides that a business cannot discriminate against a consumer for exercising his or her CCPA rights, except that a business may offer a different price, rate, level or quality of goods or services to the consumer if the differential treatment is reasonably related to the value provided *to the consumer* by the consumer's data. **AB 1355** would revise that language to clarify permissible discrimination must be reasonably related to the value provided *to the business* by the consumer's data.

Updates to the Definition of Personal Information

Three bills would make a variety of changes to the definition of personal information under the Act.

Information Must Be *Reasonably* Associated with an Individual. **AB 874** would revise the definition of "personal information" to add a reasonable requirement to information that could be associated with a particular individual or household. If signed, personal information would be defined as information that identifies, relates to, describes, is *reasonably* capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Unrestricted Use of Publicly Available Government Records. While the CCPA excludes from the definition of "personal information" data that is lawfully made available from federal, state or local records, existing law specifies that such information is not "publicly available" if it is used for a purpose that is not compatible with the purpose for which such information is maintained. If signed,

AB 874 would delete that use restriction and instead provide that "publicly available" information is simply information that is lawfully made available from federal, state or local records.

Clarification on Use of Deidentified or Aggregate Information. **AB 874** and **AB 1355** would each correct an apparent typo in the existing law and clarify that deidentified or aggregate consumer information is not "personal information" (rather than not "publicly available" information as stated in the existing law).

Surprise Failure: Bill to Protect Loyalty Programs Doesn't Come Up for Vote

The big surprise last week was that the bill to expressly protect loyalty programs, **AB 846**, was pulled from consideration and moved to the inactive file.

The bill was introduced to address a concern raised by businesses that a consumer's deletion request could require the deletion of loyalty program data and perks, a result that 1) at least arguably would conflict with the CCPA's anti-discrimination provision and 2) runs contrary to marketing departments' typical desire to keep people enrolled.

Support by companies dwindled, however, after the Senate Judiciary Committee forced an amendment that would have limited how businesses could use data collected in connection with a loyalty program. Privacy advocates never got behind the bill, pointing to the various exemptions from deletion found in the CCPA, and the fact that the Act permits a business to provide a different price or quality of goods if the difference is reasonably related to the value provided to the business by the consumer's data.

What Happens Next?

Gov. Newsom has until Oct. 13, 2019, to sign or veto the legislation, and the order in which he enacts bills will determine whether some overlapping provisions of the bills are enacted or not.

Further complicating companies' efforts to operationalize the CCPA is the fact that regulations are still forthcoming. The state attorney general is expected to release draft regulations sometime this fall.

California Leading the Way on Privacy

In the absence of comprehensive federal privacy legislation, California has moved forward on its own, and the CCPA will come into effect alongside a number of other generally pro-consumer privacy laws.

Data Broker Registry. If signed, **AB 1202** would establish a public registry of names, addresses and contact information for data brokers — companies that knowingly collect and sell the personal information of California consumers with whom they do not have a direct relationship. (The bill incorporates the broad definitions of "collect," "sell" and "personal information" as used in CCPA.)

Exempted from the definition of a data broker are:

1. a consumer reporting agency to the extent that it is covered by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 *et seq.*)
2. a financial institution to the extent that it is covered by the Gramm-Leach-Bliley Act (Public Law 106-102) and implementing regulations

3. an entity to the extent that it is covered by the Insurance Information and Privacy Protection Act (Article 6.6 (commencing with Section 1791) of Chapter 1 of Part 2 of Division 1 of the Insurance Code)

On or before Jan. 31 following each year in which a business meets the definition of data broker, a business would have to register with the state attorney general's office and pay a fee. A data broker who fails to register would be subject to an injunction and civil penalties ($100 per day), fees and costs in an action brought by the attorney general.

Unlike Vermont's data broker law, the California law does not include standalone information security or computer system security requirements. However, the registry would exist alongside the CCPA, which imposes a general duty on all businesses to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information collected and used. Cal. Civ. Code § 1798.150.

Other California privacy laws coming into effect on Jan. 1, 2020, include:

Security of Connected Devices, California Civil Code §§ 1798.91.04, will ban "default" passwords for connected devices, and require manufacturers to equip such devices with reasonable security features appropriate to the nature of the device and the information collected.

Parent's Accountability and Child Protection Act, California Civil Code §§ 1798.99 *et seq.*, will require an entity that conducts business in California to take reasonable steps to ensure that the purchaser of select goods or services is of legal age at the time of the purchase.

If signed by Gov. Newsom, **AB 1138** would amend the Parent's Accountability and Child Protection Act to require a business that operates a social media website or application to obtain consent from the parent or guardian of its users under age 13, beginning July 1, 2021.

For additional information regarding the CCPA or the latest developments detailed in this alert, contact the author.

Author

Ashley L. Shively
San Francisco
415.743.6906
ashley.shively@hklaw.com

Holland & Knight

California Attorney General Releases Draft Regulations on the California Consumer Privacy Act

New Requirements Have Potentially Significant Impact on the Provision of Notice and Administration of Customer Loyalty Programs

October 31, 2019

Holland & Knight Alert

Ashley L. Shively | Mark S. Melodia | Marissa C. Serafino

Highlights

- The California Attorney General Xavier Becerra on Oct. 10, 2019, released the proposed text for the California Consumer Privacy Act (CCPA) Regulations. The following day, Gov. Gavin Newsom signed into law five amendments to the Act, and laws to regulate data brokers and social media accounts.
- The proposed regulations are intended to guide businesses on how to comply with CCPA with a focus on notices to consumers, business practices for handling consumer requests, verification of requests, special rules regarding minors and nondiscrimination.
- Public comments on the draft regulations are due on Dec. 6, 2019, at 5 p.m. PST. The Attorney General will hold four public hearings to address the regulations during the first week of December.

The California Attorney General Xavier Becerra on Oct. 10, 2019, released the proposed text for the California Consumer Privacy Act Regulations (Regulations). The Regulations are intended to guide businesses on CCPA compliance with a focus on five areas: notices to consumers, business practices for handling consumer requests, verification of requests, special rules regarding minors and nondiscrimination. The following day, Gov. Gavin Newsom signed into law five amendments to the Act, and laws to regulate data brokers and social media accounts. (See Holland & Knight's previous alert, "Hospitality Industry Prepares for Slate of New Consumer Privacy Protections," Oct. 7, 2019.)

Industry has until Dec. 6, 2019, to submit comments on the Regulations, and the Attorney General will hold four public hearings to address the Regulations, on Dec. 2 in Sacramento, Dec. 3 in Los Angeles, Dec. 4 in San Francisco and Dec. 5 in Fresno. While CCPA becomes operational on Jan. 1, 2020, enforcement of the law will not occur until the regulations have been finalized, but no later than July 1, 2020.

This Holland & Knight alert provides a detailed look at some of the key takeaways from the Regulations. Given the potential confusion and uncertainty presented by the CCPA and these Regulations, please contact the authors should your organization require assistance.

CCPA's Proposed Regulations: Key Takeaways

Consumer Notice Separate from Privacy Policy?

Many businesses had interpreted CCPA's notice requirement as satisfied through provision of a privacy policy. The Regulations, however, introduce ambiguity around consumer disclosures by discussing notice requirements separately from a privacy policy. § 999.305(c). This raises operational questions related to the provision of notice that are unanswered in the Regulations. In response, some businesses may elect to proceed with a separate stand-alone notice, perhaps as a pop-up or banner, which directs consumers to a linked privacy policy.

An "Easy to Read" Notice Could be a Tall Order

The Regulations emphasize that both notices and privacy policies should be straightforward and in "plain English" in order to provide consumers with a clear description of a business' online and offline practices regarding collection, use, disclosure and sale of personal information, and also explain consumers' access and request rights.

That instruction is in tension with the complicated definitions that CCPA assigns to key terms. For instance, because "sale" is defined under Civil Code Section 1798.140(t)(1) more broadly than that word is normally used or understood, a business may reasonably struggle to explain its practices in language familiar to consumers.

Drafting a "plain English" disclosure is all the more challenging given the level of granularity that the Regulations specify must be included in notices to consumers and a company's privacy policy. A privacy policy alone, for instance, is now required to:

- list the categories of personal information (which alone is defined to include 30-plus data points under Civil Code Section 1798.140(o)(1)) that the business has collected about consumers in the prior 12 months, § 999.308(b)(1)(d)(1)
- for each category of personal information, provide: 1) the "categories of sources" from which the information was collected, 2) the business or commercial purpose for which the information was collected, and 3) the categories of third parties with whom the business shares personal information, § 999.308(b)(1)(d)(2)
- explain that a consumer has the right to request that the business disclose what categories of personal information it collects, uses, discloses and sells, and to share the information specific to the consumer held by the business, § 999.308(b)(1)-(3)
- explain that a consumer has the right to request that the business delete his or her personal information
- explain that a consumer has the right to request that the business not sell his or her personal information to third parties
- explain that a consumer has the right not to be discriminated against for exercising his or her rights under the CCPA, § 999.308(b)(4)
- describe how a consumer can submit a request exercising his or her rights and the process that the business will use to verify such request, including any information the consumer, or his or her authorized agent, will need to provide, § 999.308(b)(1); § 999.308(b)(5)
- explain any financial incentive or price or service difference offered by the business, and why it is reasonably related to the value of the consumer's data to the business, § 999.305(b); § 999.336(e)

In addition:

- If an incentive is offered, a business must further provide a good faith estimate of the value of the consumer's data and a description of the method used to calculate that amount. § 999.307(b)(5)
- Despite the Act's prohibition against selling the personal information of minors without affirmative authorization [Civil Code § 1798.120(d)], the Regulations require a business to state whether or not it sells personal information of minors under 16 years of age without affirmative authorization. § 999.308(b)(1)(e)(3)

The Regulations Complicate Administration of Customer Loyalty Programs

The CCPA prohibits a business from discriminating against consumers — denying goods or services, charging different prices or rates for goods or services, or providing a different level or quality of goods or services to the consumer — for exercising their rights under CCPA. Civil Code § 1798.125. The Act includes an exception however. A

business may offer a financial incentive or price or service difference in exchange for retention or sale of a consumer's personal information, provided that the incentive or price or service difference is *reasonably related to the value of the consumer's data*. Civil Code § 1798.125(a)(2) (as amended in AB 1355); Reg. § 999.336(a)-(b)

A few examples are illustrative:

1. A hotel offers standard-speed Wi-Fi for free and a premium service that costs $5 per night. If only the consumers who pay for Wi-Fi are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5 per night payment is reasonably related to the value of the consumer's data to the business.
2. An amusement park offers discounted prices to consumers who sign up to be on its mailing list. If the consumer on the mailing list can continue to receive discounted ticket prices even after she has made a request to know, request to delete, and/or request to opt-out, the differing price level is not discriminatory.

See Reg. § 999.336(c)

Calculating "the value of the consumer's data" presents its own challenge. The Regulations list eight methods of calculation. § 999.337(b). The broadest permissible method — "any other practical and reliable method of calculation used in good-faith" — would seem to offer businesses flexibility, but it also gives the Attorney General significant authority to interpret how it is applied.

Changes to Business Practices

The Regulations include new requirements and restrictions that a business must consider in complying with the CCPA, including responding to consumer requests, training employees and record keeping. The following are key changes to business practices that are described in the Regulations:

- Responding to Consumer Requests: A business is prohibited from providing certain data elements in response to consumer access requests, if disclosure creates a "substantial, articulable and unreasonable risk of security" to the personal information, the consumer's account, or the security of the business' systems. § 999.313(c)(3). Though this standard is not defined in the CCPA or the Regulations, businesses will need to have a mechanism for determining whether disclosure of data would meet this threshold and providing an appropriate response to a consumer request. The Regulations also prohibit a business from providing a social security number, driver's license, financial account number, health insurance/medical ID number, account password, security questions/answers in responding to an access request. § 999.313(c)(3)-(4)
- Training: Business must provide training on the CCPA and the Regulations to individuals responsible for handling the business' consumer inquiries. § 999.317(a)
- Record keeping: The Regulations also include new record-keeping requirements. A business must maintain records of consumer requests and how it responded for 24 months. § 999.317(b), (c). Additional record keeping and disclosure requirements exist for businesses that annually buy, receive, sell or share the personal information of ***4 million*** or more consumers. § 999.317(g). The Regulations provide no guidance about how to determine the number of consumers touched by a business. It is unclear, for instance, whether a business must count all subscribers to marketing emails separately from social media engagement, even though there is likely substantial overlap between the two groups. Or would a business be required to take steps to reconcile various databases and pinpoint geography for those users, in order to make a good faith determination that the 4 million threshold does not apply.

Either way, a business that meets the 4 million consumer threshold must:

1. compile for the previous calendar year a) the number of requests to know that the business received, complied with

in whole or in part, and denied; b) the number of requests to delete that the business received, complied with in whole or in part, and denied; c) the number of requests to opt-out that the business received, complied with in whole or in part, and denied; and d) the median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

2. disclose the compiled information within the business' privacy policy *or* post it on the business' website and make the information accessible from a link included in their privacy policy.
3. establish, document and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business' compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

See § 999.317(g).

Do Not Sell Requirements

While the State Attorney General has yet to release details regarding the appearance of the Do Not Sell button, the Regulations do provide guidance and clarity on the Act's opt-out requirement, and the new requirement to opt a consumer back in after a business processes an earlier Do Not Sell request.

1. "Do Not Sell" Requirements: Under the CCPA, a business is required to provide two or more methods for consumers to submit requests to opt-out, "including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled 'Do Not Sell My Personal Information,' or 'Do Not Sell My Info,' on the business's website or mobile application." Civil Code § 1798.135. A business can offer additional methods for submitting these requests, such as a designated email address, but at least one of the methods must reflect the manner in which the business primarily interacts with the consumer.
2. Do Not Track: User-enabled privacy controls, such as a browser plugin or privacy setting, that signal a consumer's choice to opt-out of the sale of their personal information constitute a valid and direct opt-out request for that browser, device or consumer. § 999.315(c). Given the absence of an industry standard as to how such "signals" work or are communicated, however, it is unclear how this new requirement can be implemented with any consistency.
3. Authorized Agent: A consumer may use an authorized agent to submit a request to opt-out by providing the authorized agent with written permission. A business may deny a request from an agent who does not submit proof that he or she is authorized to act on the consumer's behalf. § 999.315(g).
4. Key Timing Requirements: A business must act upon a request to opt-out no later than 15 days from receipt. § 999.315(e). A business must also notify all third parties to whom it has sold the consumer's personal information within 90 days from when the business received the consumer's opt-out request and instruct them not to further sell the information, and notify the consumer when this has been completed. § 999.315(f).
5. Unverified Requests: Opt-out requests need not be a "verifiable consumer request." A business, however, may deny a request if it has a good-faith and reasonable belief the request is fraudulent. § 999.315(h). That decision should be documented, and the business should inform the requesting party that the request has been denied and provide an explanation for why the business believes the request is fraudulent.
6. Consequences for Omitting Do Not Sell Link: If a business states in its privacy policy that it "does not sell" personal information, or if it does not have a Do Not Sell link on its website, consumers are deemed to have validly submitted a request to opt-out. § 999.306(d)(2). Practically speaking, this means that a business could not later decide to "sell" consumers' personal information without first obtaining a clear confirmation from the consumer of his or her new choice to opt in.

7. Two-Step Process for Opting-In After a Prior Opt-Out: Businesses must use a two-step opt-in process for the sale of personal information whereby the consumer clearly requests to opt-in, and then separately confirms his or her choice. A business is allowed to inform a consumer who has opted-out that a transaction requires the sale of their personal information as a condition of completing the transaction and provide instructions for opting-in. § 999.316(a)-(b)
8. Third Party Obligations Before Reselling Personal Information: A company that resells personal information received from a CCPA-covered business, must, before it sells personal information: 1) contact the consumer directly to give notice that it sells personal information about the consumer and provide an opportunity for the consumer to opt-out; or 2) contact the business and confirm notice and an opportunity to opt-out was provided to the consumer at the point of collection, and obtain a signed attestation from the collecting business describing how it gave notice and an example of such notice. The third party must maintain the attestation for two years and make it available to the consumer upon request. § 999.305(d)

Requests to Access or Delete Household Information

The Regulations clean up a definitional gap in CCPA and define "household" as a person or group of people occupying a single dwelling. § 999.301(h). If a consumer does not have a password-protected account with the business, a business may respond to a request to know or delete as it relates to the household by providing aggregate personal information (subject to verification requirements detailed below). A business must comply with such a request if all consumers of the household jointly request access to specific pieces or deletion of household personal information, and the business can individually verify all members of the household. § 999.318(a)-(b). Treating consumers as individuals and as part of a group could cause confusion and duplication regarding requests and responses.

Verifying Consumer Requests

The Regulations detail stringent requirements for verification of consumer requests. A business is required to establish a method to verify the identity of consumers making access or deletion requests. § 999.323(a). This can include matching identifying information provided by the consumer to the personal information held by the business or by using a third-party identity verification service. § 999.323(b)(1). Alternatively, a business can verify a consumer's identity through existing authentication practices for the consumer's password-protected account, as long as the consumer re-authenticates themselves before a business discloses or deletes data. § 999.324(a).

A business must deny a consumer's request, however, if it suspects fraudulent or malicious activity on or from the password-protected account, which places the onus businesses to make a determination about what should be considered suspect activity. § 999.324(a)-(b). If a business has no reasonable method to verify the identity of the consumer, the business may decline the request and must explain why in its response. § 999.325(f).

In keeping with the principles of CCPA, businesses are encouraged to minimize data collection for verification purposes and protect consumer data. § 999.323(c). Specifically, businesses are required to implement "reasonable security measures" to detect fraudulent identity-verification activity and prevent unauthorized access to a consumer's personal information. § 999.323(d). What constitutes "reasonable security measures" will likely depend on the personal information held by a business.

Conclusion

While these proposed Regulations offer guidance about how businesses can comply with CCPA, it remains unclear how California's Attorney General will interpret and enforce key CCPA provisions. The Attorney General is expected to secure additional funding in the coming years to support staff dedicated to CCPA. However, the 2020 ballot measure on privacy proposed by Alastair Mactaggart in September 2019 adds another element of uncertainty for businesses determining compliance strategies.

Holland & Knight

Despite this uncertainty, companies should use the next 60 days before the law becomes operational on Jan. 1, 2020, to become familiar with the CCPA and these Regulations, identify questions and gaps posed by the law, develop and implement compliance plans, and to train employees.

Authors

Ashley L. Shively is a class action litigator and privacy attorney in Holland & Knight's San Francisco office. She focuses her litigation practice on the defense of financial institutions and businesses in consumer class and individual actions, including fair lending, data breach, privacy, credit reporting, debt collection, false advertising and unfair business practices. Ms. Shively has extensive experience litigating class actions under the Truth in Lending Act (TILA), Telephone Consumer Protection Act (TCPA) and California's Invasion of Privacy Act (CIPA).

415.743.6906 | Ashley.Shively@hklaw.com

Mark Melodia is a privacy, data security and consumer class action defense lawyer in Holland & Knight's New York office and serves as the head of the firm's Data Strategy, Security & Privacy Team. Mr. Melodia focuses his practice on governmental and internal investigations, putative class actions and other "bet-the-company" suits in the following areas: data security/privacy, mortgage/financial services and other complex business litigation, including defamation.

212.513.3583 | Mark.Melodia@hklaw.com

Marissa Serafino is a Washington, D.C., public affairs advisor in Holland & Knight's Public Policy & Regulation Group, where she develops federal advocacy strategies for local government municipalities, nonprofits and associations. Ms. Serafino focuses on identifying innovative solutions to legislative and regulatory matters involving transportation, housing, infrastructure, judiciary and environment issues.

202.469.5414 | Marissa.Serafino@hklaw.com

TITLE 11. LAW

DIVISION 1. ATTORNEY GENERAL

CHAPTER 20. CALIFORNIA CONSUMER PRIVACY ACT REGULATIONS

PROPOSED TEXT OF REGULATIONS

Article 1. General Provisions

§ 999.300. Title and Scope

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

§ 999.301. Definitions

In addition to the definitions set forth in Civil Code section 1798.140, for purposes of these regulations:

(a) "Affirmative authorization" means an action that demonstrates the intentional decision by the consumer to opt-in to the sale of personal information. Within the context of a parent or guardian acting on behalf of a child under 13, it means that the parent or guardian has provided consent to the sale of the child's personal information in accordance with the methods set forth in section 999.330. For consumers 13 years and older, it is demonstrated through a two-step process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) "Attorney General" means the California Attorney General or any officer or employee of the California Department of Justice acting under the authority of the California Attorney General.

(c) "Authorized agent" means a natural person or a business entity registered with the Secretary of State that a consumer has authorized to act on their behalf subject to the requirements set forth in section 999.326.

(d) "Categories of sources" means types of entities from which a business collects personal information about consumers, including but not limited to the consumer directly, government entities from which public records are obtained, and consumer data resellers.

(e) "Categories of third parties" means types of entities that do not collect personal information directly from consumers, including but not limited to advertising networks, internet service providers, data analytics providers, government entities, operating systems and platforms, social networks, and consumer data resellers.

(f) "CCPA" means the California Consumer Privacy Act of 2018, Civil Code sections 1798.100 *et seq.*

(g) "Financial incentive" means a program, benefit, or other offering, including payments to consumers as compensation, for the disclosure, deletion, or sale of personal information.

(h) "Household" means a person or group of people occupying a single dwelling.

(i) "Notice at collection" means the notice given by a business to a consumer at or before the time a business collects personal information from the consumer as required by Civil Code section 1798.100(b) and specified in these regulations.

(j) "Notice of right to opt-out" means the notice given by a business informing consumers of their right to opt-out of the sale of their personal information as required by Civil Code sections 1798.120 and 1798.135 and specified in these regulations.

(k) "Notice of financial incentive" means the notice given by a business explaining each financial incentive or price or service difference subject to Civil Code section 1798.125(b) as required by that section and specified in these regulations.

(l) "Price or service difference" means (1) any difference in the price or rate charged for any goods or services to any consumer, including through the use of discounts, financial payments, or other benefits or penalties; or (2) any difference in the level or quality of any goods or services offered to any consumer, including denial of goods or services to the consumer.

(m) "Privacy policy" means the policy referred to in Civil Code section 1798.130(a)(5), and means the statement that a business shall make available to consumers describing the business's practices, both online and offline, regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their own personal information.

(n) "Request to know" means a consumer request that a business disclose personal information that it has about the consumer pursuant to Civil Code sections 1798.100, 1798.110, or 1798.115. It includes a request for any or all of the following:

(1) Specific pieces of personal information that a business has about the consumer;

(2) Categories of personal information it has collected about the consumer;

(3) Categories of sources from which the personal information is collected;

(4) Categories of personal information that the business sold or disclosed for a business purpose about the consumer;

(5) Categories of third parties to whom the personal information was sold or disclosed for a business purpose; and

(6) The business or commercial purpose for collecting or selling personal information.

(o) "Request to delete" means a consumer request that a business delete personal information about the consumer that the business has collected from the consumer, pursuant to Civil Code section 1798.105.

(p) "Request to opt-out" means a consumer request that a business not sell the consumer's personal information to third parties, pursuant to Civil Code section 1798.120(a).

(q) "Request to opt-in" means the affirmative authorization that the business may sell personal information about the consumer required by Civil Code section 1798.120(c) by a parent or guardian of a consumer less than 13 years of age, or by a consumer who had previously opted out of the sale of their personal information.

(r) "Third-party identity verification service" means a security process offered by an independent third party who verifies the identity of the consumer making a request to the business. Third-party verification services are subject to the requirements set forth in Article 4 regarding requests to know and requests to delete.

(s) "Typical consumer" means a natural person residing in the United States.

(t) "URL" stands for Uniform Resource Locator and refers to the web address of a specific website.

(u) "Verify" means to determine that the consumer making a request to know or request to delete is the consumer about whom the business has collected information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100-1798.199, Civil Code.

Article 2. Notices to Consumers

§ 999.305. Notice at Collection of Personal Information

(a) Purpose and General Principles

(1) The purpose of the notice at collection is to inform consumers at or before the time of collection of a consumer's personal information of the categories of personal information to be collected from them and the purposes for which the categories of personal information will be used.

(2) The notice at collection shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

e. Be visible or accessible where consumers will see it before any personal information is collected. For example, when a business collects consumers' personal information online, it may conspicuously post a link to the notice on the business's website homepage or the mobile application's download page, or on all webpages where personal information is collected. When a business collects consumers' personal information offline, it may, for example, include the notice on printed forms that collect personal information, provide the consumer with a paper version of the notice, or post prominent signage directing consumers to the web address where the notice can be found.

(3) A business shall not use a consumer's personal information for any purpose other than those disclosed in the notice at collection. If the business intends to use a consumer's personal information for a purpose that was not previously disclosed to the consumer in the notice at collection, the business shall directly notify the consumer of this new use and obtain explicit consent from the consumer to use it for this new purpose.

(4) A business shall not collect categories of personal information other than those disclosed in the notice at collection. If the business intends to collect additional categories of personal information, the business shall provide a new notice at collection.

(5) If a business does not give the notice at collection to the consumer at or before the collection of their personal information, the business shall not collect personal information from the consumer.

(b) A business shall include the following in its notice at collection:

(1) A list of the categories of personal information about consumers to be collected. Each category of personal information shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

(2) For each category of personal information, the business or commercial purpose(s) for which it will be used.

(3) If the business sells personal information, the link titled "Do Not Sell My Personal Information" or "Do Not Sell My Info" required by section 999.315(a), or in the case of offline notices, the web address for the webpage to which it links.

(4) A link to the business's privacy policy, or in the case of offline notices, the web address of the business's privacy policy.

(c) If a business collects personal information from a consumer online, the notice at collection may be given to the consumer by providing a link to the section of the business's privacy policy that contains the information required in subsection (b).

(d) A business that does not collect information directly from consumers does not need to provide a notice at collection to the consumer, but before it can sell a consumer's personal information, it shall do either of the following:

(1) Contact the consumer directly to provide notice that the business sells personal information about the consumer and provide the consumer with a notice of right to opt-out in accordance with section 999.306; or

(2) Contact the source of the personal information to:

a. Confirm that the source provided a notice at collection to the consumer in accordance with subsections (a) and (b); and

b. Obtain signed attestations from the source describing how the source gave the notice at collection and including an example of the notice. Attestations shall be retained by the business for at least two years and made available to the consumer upon request.

Note: Authority: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.115, and 1798.185, Civil Code.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information

(a) Purpose and General Principles

(1) The purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future.

(2) The notice of right to opt-out shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

(b) A business that sells the personal information of a consumer shall provide a notice of right to opt-out to the consumer as follows:

(1) A business shall post the notice of right to opt-out on the Internet webpage to which the consumer is directed after clicking on the "Do Not Sell My Personal Information" or "Do Not Sell My Info" link on the website homepage or the download or landing page of a mobile application. The notice shall include the information specified in

subsection (c) or link to the section of the business's privacy policy that contains the same information.

(2) A business that substantially interacts with consumers offline shall also provide notice to the consumer by an offline method that facilitates consumer awareness of their right to opt-out. Such methods include, but are not limited to, printing the notice on paper forms that collect personal information, providing the consumer with a paper version of the notice, and posting signage directing consumers to a website where the notice can be found.

(3) A business that does not operate a website shall establish, document, and comply with another method by which it informs consumers of their right to direct a business that sells their personal information to stop selling their personal information. That method shall comply with the requirements set forth in subsection (a)(2).

(c) A business shall include the following in its notice of right to opt-out:

(1) A description of the consumer's right to opt-out of the sale of their personal information by the business;

(2) The webform by which the consumer can submit their request to opt-out online, as required by Section 999.315(a), or if the business does not operate a website, the offline method by which the consumer can submit their request to opt-out;

(3) Instructions for any other method by which the consumer may submit their request to opt-out;

(4) Any proof required when a consumer uses an authorized agent to exercise their right to opt-out, or in the case of a printed form containing the notice, a webpage, online location, or URL where consumers can find information about authorized agents; and

(5) A link or the URL to the business's privacy policy, or in the case of a printed form containing the notice, the URL of the webpage where consumers can access the privacy policy.

(d) A business is exempt from providing a notice of right to opt-out if:

(1) It does not, and will not, sell personal information collected during the time period during which the notice of right to opt-out is not posted; and

(2) It states in its privacy policy that that it does not and will not sell personal information. A consumer whose personal information is collected while a notice of right to opt-out notice is not posted shall be deemed to have validly submitted a request to opt-out.

(e) Opt-Out Button or Logo

(1) The following opt-out button or logo may be used in addition to posting the notice of right to opt-out, but not in lieu of any posting of the notice. [BUTTON OR LOGO TO BE ADDED IN A MODIFIED VERSION OF THE REGULATIONS AND MADE AVAILABLE FOR PUBLIC COMMENT.]

(2) This opt-out button or logo shall link to a webpage or online location containing the information specified in section 999.306(c), or to the section of the business's privacy policy that contains the same information.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135 and 1798.185, Civil Code.

§ 999.307. Notice of Financial Incentive

(a) Purpose and General Principles

(1) The purpose of the notice of financial incentive is to explain to the consumer each financial incentive or price or service difference a business may offer in exchange for the retention or sale of a consumer's personal information so that the consumer may make an informed decision on whether to participate.

(2) The notice of financial incentive shall be designed and presented to the consumer in a way that is easy to read and understandable to an average consumer. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that draws the consumer's attention to the notice and makes the notice readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the notice in an alternative format.

e. Be available online or other physical location where consumers will see it before opting into the financial incentive or price or service difference.

(3) If the business offers the financial incentive or price of service difference online, the notice may be given by providing a link to the section of a business's privacy policy that contains the information required in subsection (b).

(b) A business shall include the following in its notice of financial incentive:

(1) A succinct summary of the financial incentive or price or service difference offered;

(2) A description of the material terms of the financial incentive or price of service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference;

(3) How the consumer can opt-in to the financial incentive or price or service difference;

(4) Notification of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and

(5) An explanation of why the financial incentive or price or service difference is permitted under the CCPA, including:

a. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and

b. A description of the method the business used to calculate the value of the consumer's data.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125 and 1798.130, Civil Code.

§ 999.308. Privacy Policy

(a) Purpose and General Principles

(1) The purpose of the privacy policy is to provide the consumer with a comprehensive description of a business's online and offline practices regarding the collection, use, disclosure, and sale of personal information and of the rights of consumers regarding their personal information. The privacy policy shall not contain specific pieces of personal information about individual consumers and need not be personalized for each consumer.

(2) The privacy policy shall be designed and presented in a way that is easy to read and understandable to an average consumer. The notice shall:

a. Use plain, straightforward language and avoid technical or legal jargon.

b. Use a format that makes the policy readable, including on smaller screens, if applicable.

c. Be available in the languages in which the business in its ordinary course provides contracts, disclaimers, sale announcements, and other information to consumers.

d. Be accessible to consumers with disabilities. At a minimum, provide information on how a consumer with a disability may access the policy in an alternative format.

e. Be available in an additional format that allows a consumer to print it out as a separate document.

(3) The privacy policy shall be posted online through a conspicuous link using the word "privacy," on the business's website homepage or on the download or landing page of a mobile application. If the business has a California-specific description of consumers' privacy rights on its website, then the privacy policy shall be included in that description. A business that does not operate a website shall make the privacy policy conspicuously available to consumers.

(b) The privacy policy shall include the following information:

(1) Right to Know About Personal Information Collected, Disclosed, or Sold

a. Explain that a consumer has the right to request that the business disclose what personal information it collects, uses, discloses, and sells.

b. Provide instructions for submitting a verifiable consumer request to know and provide links to an online request form or portal for making the request, if offered by the business.

c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.

d. Collection of Personal Information

1. List the categories of consumers' personal information the business has collected about consumers in the preceding 12 months. The notice shall be written in a manner that provides consumers a meaningful understanding of the information being collected.

2. For each category of personal information collected, provide the categories of sources from which that information was collected, the business or commercial purpose(s) for which the information was collected, and the categories of third parties with whom the business shares personal information. The notice shall be written in a manner that provides consumers a meaningful understanding of the categories listed.

e. Disclosure or Sale of Personal Information

1. State whether or not the business has disclosed or sold any personal information to third parties for a business or commercial purpose in the preceding 12 months.

2. List the categories of personal information, if any, that it disclosed or sold to third parties for a business or commercial purpose in the preceding 12 months.

3. State whether or not the business sells the personal information of minors under 16 years of age without affirmative authorization.

(2) Right to Request Deletion of Personal Information

a. Explain that the consumer has a right to request the deletion of their personal information collected or maintained by the business.

b. Provide instructions for submitting a verifiable consumer request to delete and provide links to an online request form or portal for making the request, if offered by the business.

c. Describe the process the business will use to verify the consumer request, including any information the consumer must provide.

(3) Right to Opt-Out of the Sale of Personal Information

a. Explain that the consumer has a right to opt-out of the sale of their personal information by a business.

b. Include the contents of the notice of right to opt-out or a link to it in accordance with section 999.306.

(4) Right to Non-Discrimination for the Exercise of a Consumer's Privacy Rights

a. Explain that the consumer has a right not to receive discriminatory treatment by the business for the exercise of the privacy rights conferred by the CCPA.

(5) Authorized Agent

a. Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf.

(6) Contact for More Information: Provide consumers with a contact for questions or concerns about the business's privacy policies and practices using a method reflecting the manner in which the business primarily interacts with the consumer.

(7) Date the privacy policy was last updated.

(8) If subject to the requirements set forth section 999.317(g), the information compiled in section 999.317(g)(1) or a link to it.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.115, 1798.120, 1798.125 and 1798.130, Civil Code.

Article 3. Business Practices for Handling Consumer Requests

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete

(a) A business shall provide two or more designated methods for submitting requests to know, including, at a minimum, a toll-free telephone number, and if the business operates a website, an interactive webform accessible through the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a designated email address, a form submitted in person, and a form submitted through the mail.

(b) A business shall provide two or more designated methods for submitting requests to delete. Acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a link or form available online through a business's website, a designated email address, a form submitted in person, and a form submitted through the mail.

(c) A business shall consider the methods by which it interacts with consumers when determining which methods to provide for submitting requests to know and requests to delete. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer, even if it requires a business to offer three methods for submitting requests to know. Illustrative examples follow:

(1) *Example 1:* If the business is an online retailer, at least one method by which the consumer may submit requests should be through the business's retail website.

(2) *Example 2:* If the business operates a website but primarily interacts with customers in person at a retail location, the business shall offer three methods to submit requests to know—a toll-free telephone number, an interactive webform accessible through the business's website, and a form that can be submitted in person at the retail location.

(d) A business shall use a two-step process for online requests to delete where the consumer must first, clearly submit the request to delete and then second, separately confirm that they want their personal information deleted.

(e) If a business does not interact directly with consumers in its ordinary course of business, at least one method by which a consumer may submit requests to know or requests to delete shall be online, such as through the business's website or a link posted on the business's website.

(f) If a consumer submits a request in a manner that is not one of the designated methods of submission, or is deficient in some manner unrelated to the verification process, the business shall either:

(1) Treat the request as if it had been submitted in accordance with the business's designated manner, or

(2) Provide the consumer with specific directions on how to submit the request or remedy any deficiencies with the request, if applicable.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.313. Responding to Requests to Know and Requests to Delete

(a) Upon receiving a request to know or a request to delete, a business shall confirm receipt of the request within 10 days and provide information about how the business will process the request. The information provided shall describe the business's verification process and when the consumer should expect a response, except in instances where the business has already granted or denied the request.

(b) Businesses shall respond to requests to know and requests to delete within 45 days. The 45-day period will begin on the day that the business receives the request, regardless of time required to verify the request. If necessary, businesses may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received, provided that the business provides the consumer with notice and an explanation of the reason that the business will take more than 45 days to respond to the request.

(c) Responding to Requests to Know

(1) For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the consumer that it cannot verify their identity. If the request is denied in whole or in part, the business shall also evaluate the consumer's request as if it is seeking the disclosure of categories of personal information about the consumer pursuant to subsection (c)(2).

(2) For requests that seek the disclosure of categories of personal information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business may deny the request to disclose the categories and other information requested and shall inform the requestor that it cannot verify their identity. If the request is denied in whole or in part, the business shall provide or direct the consumer to its general business practices regarding the collection, maintenance, and sale of personal information set forth in its privacy policy.

(3) A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks.

(4) A business shall not at any time disclose a consumer's Social Security number, driver's license number or other government-issued identification number, financial account number, any health insurance or medical identification number, an account password, or security questions and answers.

(5) If a business denies a consumer's verified request to know specific pieces of personal information, in whole or in part, because of a conflict with federal or state law, or an exception to the CCPA, the business shall inform the requestor and explain the basis for the denial. If the request is denied only in part, the business shall disclose the other information sought by the consumer.

(6) A business shall use reasonable security measures when transmitting personal information to the consumer.

(7) If a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal for consumers to access, view, and receive a portable copy of their personal information if the portal fully discloses the personal information that the consumer is entitled to under the CCPA and these regulations, uses reasonable data security controls, and complies with the verification requirements set forth in Article 4.

(8) Unless otherwise specified, the 12-month period covered by a consumer's verifiable request to know referenced in Civil Code section 1798.130(a)(2) shall run from the

date the business receives the request, regardless of the time required to verify the request.

(9) In responding to a consumer's verified request to know categories of personal information, categories of sources, and/or categories of third parties, a business shall provide an individualized response to the consumer as required by the CCPA. It shall not refer the consumer to the businesses' general practices outlined in its privacy policy unless its response would be the same for all consumers and the privacy policy discloses all the information that is otherwise required to be in a response to a request to know such categories.

(10) In responding to a verified request to know categories of personal information, the business shall provide for each identified category of personal information it has collected about the consumer:

a. The categories of sources from which the personal information was collected;

b. The business or commercial purpose for which it collected the personal information;

c. The categories of third parties to whom the business sold or disclosed the category of personal information for a business purpose; and

d. The business or commercial purpose for which it sold or disclosed the category of personal information.

(11) A business shall identify the categories of personal information, categories of sources of personal information, and categories of third parties to whom a business sold or disclosed personal information, in a manner that provides consumers a meaningful understanding of the categories listed.

(d) Responding to Requests to Delete

(1) For requests to delete, if a business cannot verify the identity of the requestor pursuant to the regulations set forth in Article 4, the business may deny the request to delete. The business shall inform the requestor that their identity cannot be verified and shall instead treat the request as a request to opt-out of sale.

(2) A business shall comply with a consumer's request to delete their personal information by:

a. Permanently and completely erasing the personal information on its existing systems with the exception of archived or back-up systems;

b. De-identifying the personal information; or

c. Aggregating the personal information.

(3) If a business stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system is next accessed or used.

(4) In its response to a consumer's request to delete, the business shall specify the manner in which it has deleted the personal information.

(5) In responding to a request to delete, a business shall disclose that it will maintain a record of the request pursuant to Civil Code section 1798.105(d).

(6) In cases where a business denies a consumer's request to delete the business shall do all of the following:

a. Inform the consumer that it will not comply with the consumer's request and describe the basis for the denial, including any statutory and regulatory exception therefor;

b. Delete the consumer's personal information that is not subject to the exception; and

c. Not use the consumer's personal information retained for any other purpose than provided for by that exception.

(7) In responding to a request to delete, a business may present the consumer with the choice to delete select portions of their personal information only if a global option to delete all personal information is also offered, and more prominently presented than the other choices. The business shall still use a two-step confirmation process where the consumer confirms their selection as required by section 999.312(d).

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.314. Service Providers

(a) To the extent that a person or entity provides services to a person or organization that is not a business, and would otherwise meet the requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.

(b) To the extent that a business directs a person or entity to collect personal information directly from a consumer on the business's behalf, and would otherwise meet all other requirements of a "service provider" under Civil Code section 1798.140(v), that person or entity shall be deemed a service provider for purposes of the CCPA and these regulations.

(c) A service provider shall not use personal information received either from a person or entity it services or from a consumer's direct interaction with the service provider for the purpose

of providing services to another person or entity. A service provider may, however, combine personal information received from one or more entities to which it is a service provider, on behalf of such businesses, to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity.

(d) If a service provider receives a request to know or a request to delete from a consumer regarding personal information that the service provider collects, maintains, or sells on behalf of the business it services, and does not comply with the request, it shall explain the basis for the denial. The service provider shall also inform the consumer that it should submit the request directly to the business on whose behalf the service provider processes the information and, when feasible, provide the consumer with contact information for that business.

(e) A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.315. Requests to Opt-Out

(a) A business shall provide two or more designated methods for submitting requests to opt-out, including, at a minimum, an interactive webform accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application. Other acceptable methods for submitting these requests include, but are not limited to, a toll-free phone number, a designated email address, a form submitted in person, a form submitted through the mail, and user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information.

(b) A business shall consider the methods by which it interacts with consumers when determining which methods consumers may use to submit requests to opt-out, the manner in which the business sells personal information to third parties, available technology, and ease of use by the average consumer. At least one method offered shall reflect the manner in which the business primarily interacts with the consumer.

(c) If a business collects personal information from consumers online, the business shall treat user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer.

(d) In responding to a request to opt-out, a business may present the consumer with the choice to opt-out of sales of certain categories of personal information as long as a global option to opt-out of the sale of all personal information is more prominently presented than the other choices.

(e) Upon receiving a request to opt-out, a business shall act upon the request as soon as feasibly possible, but no later than 15 days from the date the business receives the request.

(f) A business shall notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the consumer's request that the consumer has exercised their right to opt-out and instruct them not to further sell the information. The business shall notify the consumer when this has been completed.

(g) A consumer may use an authorized agent to submit a request to opt-out on the consumer's behalf if the consumer provides the authorized agent written permission to do so. A business may deny a request from an authorized agent that does not submit proof that they have been authorized by the consumer to act on the consumer's behalf. User-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information shall be considered a request directly from the consumer, not through an authorized agent.

(h) A request to opt-out need not be a verifiable consumer request. If a business, however, has a good-faith, reasonable, and documented belief that a request to opt-out is fraudulent, the business may deny the request. The business shall inform the requesting party that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent.

Note: Authority cited: Sections 1798.135 and 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, 1798.140, and 1798.185, Civil Code.

§ 999.316. Requests to Opt-In After Opting Out of the Sale of Personal Information

(a) Requests to opt-in to the sale of personal information shall use a two-step opt-in process whereby the consumer shall first, clearly request to opt-in and then second, separately confirm their choice to opt-in.

(b) A business may inform a consumer who has opted-out when a transaction requires the sale of their personal information as a condition of completing the transaction, along with instructions on how the consumer can opt-in.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.317. Training; Record-Keeping

(a) All individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CCPA shall be informed of all the requirements in the CCPA and these regulations and how to direct consumers to exercise their rights under the CCPA and these regulations.

(b) A business shall maintain records of consumer requests made pursuant to the CCPA and how the business responded to said requests for at least 24 months.

(c) The records may be maintained in a ticket or log format provided that the ticket or log includes the date of request, nature of request, manner in which the request was made, the date of the business's response, the nature of the response, and the basis for the denial of the request if the request is denied in whole or in part.

(d) A business's maintenance of the information required by this section, where that information is not used for any other purpose, does not taken alone violate the CCPA or these regulations.

(e) Information maintained for record-keeping purposes shall not be used for any other purpose.

(f) Aside from this record-keeping purpose, a business is not required to retain personal information solely for the purpose of fulfilling a consumer request made under the CCPA.

(g) A business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers, shall:

(1) Compile the following metrics for the previous calendar year:

a. The number of requests to know that the business received, complied with in whole or in part, and denied;

b. The number of requests to delete that the business received, complied with in whole or in part, and denied;

c. The number of requests to opt-out that the business received, complied with in whole or in part, and denied; and

d. The median number of days within which the business substantively responded to requests to know, requests to delete, and requests to opt-out.

(2) Disclose the information compiled in subsection (g)(1) within their privacy policy or posted on their website and accessible from a link included in their privacy policy.

(3) Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests or the business's compliance with the CCPA are informed of all the requirements in these regulations and the CCPA.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.135, and 1798.185, Civil Code.

§ 999.318. Requests to Access or Delete Household Information

(a) Where a consumer does not have a password-protected account with a business, a business may respond to a request to know or request to delete as it pertains to household personal information by providing aggregate household information, subject to verification requirements set forth in Article 4.

(b) If all consumers of the household jointly request access to specific pieces of information for the household or the deletion of household personal information, and the business can individually verify all the members of the household subject to verification requirements set forth in Article 4, then the business shall comply with the request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Section 1798.100, 1798.105, 1798.110, 1798.115, 1798.120, 1798.130, 1798.140, and 1798.185, Civil Code.

Article 4. Verification of Requests

§ 999.323. General Rules Regarding Verification

(a) A business shall establish, document, and comply with a reasonable method for verifying that the person making a request to know or a request to delete is the consumer about whom the business has collected information.

(b) In determining the method by which the business will verify the consumer's identity, the business shall:

(1) Whenever feasible, match the identifying information provided by the consumer to the personal information of the consumer already maintained by the business, or use a third-party identity verification service that complies with this section.

(2) Avoid collecting the types of personal information identified in Civil Code section 1798.81.5(d), unless necessary for the purpose of verifying the consumer.

(3) Consider the following factors:

a. The type, sensitivity, and value of the personal information collected and maintained about the consumer. Sensitive or valuable personal information shall warrant a more stringent verification process. The types of personal information identified in Civil Code section 1798.81.5(d) shall be considered presumptively sensitive;

b. The risk of harm to the consumer posed by any unauthorized access or deletion. A greater risk of harm to the consumer by unauthorized access or deletion shall warrant a more stringent verification process;

c. The likelihood that fraudulent or malicious actors would seek the personal information. The higher the likelihood, the more stringent the verification process shall be;

d. Whether the personal information to be provided by the consumer to verify their identity is sufficiently robust to protect against fraudulent requests or being spoofed or fabricated;

e. The manner in which the business interacts with the consumer; and

f. Available technology for verification.

(c) A business shall generally avoid requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, and for security or fraud-prevention purposes. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 999.317.

(d) A business shall implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information.

(e) If a business maintains consumer information that is de-identified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, 1798.140, and 1798.185, Civil Code.

§ 999.324. Verification for Password-Protected Accounts

(a) If a business maintains a password-protected account with the consumer, the business may verify the consumer's identity through the business's existing authentication practices for the consumer's account, provided that the business follows the requirements in section 999.323. The business shall also require a consumer to re-authenticate themselves before disclosing or deleting the consumer's data.

(b) If a business suspects fraudulent or malicious activity on or from the password-protected account, the business shall not comply with a consumer's request to know or request to delete until further verification procedures determine that the consumer request is authentic and the consumer making the request is the person about whom the business has collected information. The business may use the procedures set forth in section 999.325 to further verify the identity of the consumer.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.325. Verification for Non-Accountholders

(a) If a consumer does not have or cannot access a password-protected account with the business, the business shall comply with subsections (b) through (g) of this section, in addition to section 999.323.

(b) A business's compliance with a request to know categories of personal information requires that the business verify the identity of the consumer making the request to a reasonable degree of certainty. A reasonable degree of certainty may include matching at least two data points provided by the consumer with data points maintained by the business, which the business has determined to be reliable for the purpose of verifying the consumer.

(c) A business's compliance with a request to know specific pieces of personal information requires that the business verify the identity of the consumer making the request to a reasonably high degree of certainty, which is a higher bar for verification. A reasonably high degree of certainty may include matching at least three pieces of personal information provided by the consumer with personal information maintained by the business that it has determined to be reliable for the purpose of verifying the consumer together with a signed declaration under penalty of perjury that the requestor is the consumer whose personal information is the subject of the request. Businesses shall maintain all signed declarations as part of their record-keeping obligations.

(d) A business's compliance with a request to delete may require that the business verify the identity of the consumer to a reasonable degree or a reasonably high degree of certainty depending on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion. For example, the deletion of family photographs and documents may require a reasonably high degree of certainty, while the deletion of browsing history may require a reasonable degree of certainty. A business shall act in good faith when determining the appropriate standard to apply when verifying the consumer in accordance with the regulations set forth in Article 4.

(e) Illustrative scenarios follow:

(1) If a business maintains personal information in a manner associated with a named actual person, the business may verify the consumer by requiring the consumer to provide evidence that matches the personal information maintained by the business. For example, if the business maintains the consumer's name and credit card number, the business may require the consumer to provide the credit card's security code and identifying a recent purchase made with the credit card to verify their identity to reasonable degree of certainty.

(2) If a business maintains personal information in a manner that is not associated with a named actual person, the business may verify the consumer by requiring the consumer to demonstrate that they are the sole consumer associated with the non-name identifying information. This may require the business to conduct a fact-based verification process that considers the factors set forth in section 999.323(b)(3).

(f) If there is no reasonable method by which a business can verify the identity of the consumer to the degree of certainty required by this section, the business shall state so in response to any request and, if this is the case for all consumers whose personal information the business holds, in the business's privacy policy. The business shall also explain why it has no reasonable method by which it can verify the identity of the requestor. The business shall

evaluate on a yearly basis whether such a method can be established and shall document its evaluation.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

§ 999.326. Authorized Agent

(a) When a consumer uses an authorized agent to submit a request to know or a request to delete, the business may require that the consumer:

(1) Provide the authorized agent written permission to do so; and

(2) Verify their own identity directly with the business.

(b) Subsection (a) does not apply when a consumer has provided the authorized agent with power of attorney pursuant to Probate Code sections 4000 to 4465.

(c) A business may deny a request from an agent that does not submit proof that they have been authorized by the consumer to act on their behalf.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.100, 1798.110, 1798.115, 1798.130, and 1798.185, Civil Code.

Article 5. Special Rules Regarding Minors

§ 999.330. Minors Under 13 Years of Age

(a) Process for Opting-In to Sale of Personal Information

(1) A business that has actual knowledge that it collects or maintains the personal information of children under the age of 13 shall establish, document, and comply with a reasonable method for determining that the person affirmatively authorizing the sale of the personal information about the child is the parent or guardian of that child. This affirmative authorization is in addition to any verifiable parental consent required under the Children's Online Privacy Protection Act, 15 U.S.C. sections 6501, *et seq.*

(2) Methods that are reasonably calculated to ensure that the person providing consent is the child's parent or guardian include:

a. Providing a consent form to be signed by the parent or guardian under penalty of perjury and returned to the business by postal mail, facsimile, or electronic scan;

b. Requiring a parent or guardian, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder;

c. Having a parent or guardian call a toll-free telephone number staffed by trained personnel;

d. Having a parent or guardian connect to trained personnel via video-conference;

e. Having a parent or guardian communicate in person with trained personnel; and

f. Verifying a parent or guardian's identity by checking a form of government-issued identification against databases of such information, where the parent or guardian's identification is deleted by the business from its records promptly after such verification is complete.

(b) When a business receives an affirmative authorization pursuant to subsection (a) of this section, the business shall inform the parent or guardian of the right to opt-out at a later date and of the process for doing so on behalf of their child pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185(a)(6), Civil Code.

§ 999.331. Minors 13 to 16 Years of Age

(a) A business that has actual knowledge that it collects or maintains the personal information of minors at least 13 and less than 16 years of age shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information, pursuant to section 999.316.

(b) When a business receives a request to opt-in to the sale of personal information from a minor at least 13 and less than 16 years of age, the business shall inform the minor of the right to opt-out at a later date and of the process for doing so pursuant to section 999.315.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

§ 999.332. Notices to Minors Under 16 Years of Age

(a) A business subject to section 999.330 and 999.331 shall include a description of the processes set forth in those sections in its privacy policy.

(b) A business that exclusively targets offers of goods or services directly to consumers under 16 years of age and does not sell the personal information of such minors without their affirmative authorization, or the affirmative authorization of their parent or guardian for minors under 13 years of age, is not required to provide the notice of right to opt-out.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.120, 1798.135, and 1798.185, Civil Code.

Article 6. Non-Discrimination

§ 999.336. Discriminatory Practices

(a) A financial incentive or a price or service difference is discriminatory, and therefore prohibited by Civil Code section 1798.125, if the business treats a consumer differently because the consumer exercised a right conferred by the CCPA or these regulations.

(b) Notwithstanding subsection (a) of this section, a business may offer a price or service difference if it is reasonably related to the value of the consumer's data as that term is defined in section 999.337.

(c) Illustrative examples follow:

(1) *Example 1*: A music streaming business offers a free service and a premium service that costs $5 per month. If only the consumers who pay for the music streaming service are allowed to opt-out of the sale of their personal information, then the practice is discriminatory, unless the $5 per month payment is reasonably related to the value of the consumer's data to the business.

(2) *Example 2*: A retail store offers discounted prices to consumers who sign up to be on their mailing list. If the consumer on the mailing list can continue to receive discounted prices even after they have made a request to know, request to delete, and/or request to opt-out, the differing price level is not discriminatory.

(d) A business's denial of a consumer's request to know, request to delete, or request to opt-out for reasons permitted by the CCPA or these regulations shall not be considered discriminatory.

(e) A business shall notify consumers of any financial incentive or price or service difference subject to Civil Code section 1798.125 that it offers in accordance with section 999.307.

(f) A business's charging of a reasonable fee pursuant to Civil Code section 1798.145(g)(3) shall not be considered a financial incentive subject to these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

§ 999.337. Calculating the Value of Consumer Data

(a) The value provided to the consumer by the consumer's data, as that term is used in Civil Code section 1798.125, is the value provided to the business by the consumer's data and shall be referred to as "the value of the consumer's data."

(b) To estimate the value of the consumer's data, a business offering a financial incentive or price or service difference subject to Civil Code section 1798.125 shall use and document a

reasonable and good faith method for calculating the value of the consumer's data. The business shall use one or more of the following:

(1) The marginal value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;

(2) The average value to the business of the sale, collection, or deletion of a consumer's data or a typical consumer's data;

(3) Revenue or profit generated by the business from separate tiers, categories, or classes of consumers or typical consumers whose data provides differing value;

(4) Revenue generated by the business from sale, collection, or retention of consumers' personal information;

(5) Expenses related to the sale, collection, or retention of consumers' personal information;

(6) Expenses related to the offer, provision, or imposition of any financial incentive or price or service difference;

(7) Profit generated by the business from sale, collection, or retention of consumers' personal information; and

(8) Any other practical and reliable method of calculation used in good-faith.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.125, 1798.130, and 1798.185, Civil Code.

Article 7. Severability

§ 999.341.

(a) If any article, section, subsection, sentence, clause or phrase of these regulations contained in this Chapter is for any reason held to be unconstitutional, contrary to statute, exceeding the authority of the Attorney General, or otherwise inoperative, such decision shall not affect the validity of the remaining portion of these regulations.

Note: Authority cited: Section 1798.185, Civil Code. Reference: Sections 1798.105, 1798.145, 1798.185, and 1798.196, Civil Code.

CIVIL CODE - CIV[1]

DIVISION 3. OBLIGATIONS [1427 - 3273] *(Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)*

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273] *(Part 4 enacted 1872.)*

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199] *(Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)*

1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, ~~in a~~ [2]readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

(e) This section shall not require a business to retain any personal information collected for a single, one-time transaction, if such information is not sold or retained by the business or to reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 1. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.105.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

---

[1] Text reflects online version as of 9/26/19, with substantive redlines citing the applicable bill in footnotes. Note that formatting has been adjusted (tabs, spacing, etc.) for ease of reference. In addition, defined terms have a gray underline throughout; defined terms are bolded in the definitions section.

[2] AB 1355

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law,[3] provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's ~~his or her~~ right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business~~es~~' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 2. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about ~~that~~ consumers.[4]

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

[3] AB 1146
[4] AB 1355

(5) That a consumer has the right to request[5] t~~T~~he specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) The specific pieces of personal information the business has collected about that consumer.

(d) This section does not require a business to do the following:

(1) Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

(2) Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 3. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.115.

(a) A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties~~y~~[6] to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

(b) A business that sells personal information about a consumer, or that discloses a consumer's personal information for a business purpose, shall disclose, pursuant to paragraph (4) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(c) A business that sells consumers' personal information, or that discloses consumers' personal information for a business purpose, shall disclose, pursuant to subparagraph (C) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The category or categories of consumers' personal information it has sold, or if the business

[5] AB 1355
[6] AB 1355

has not sold consumers' personal information, it shall disclose that fact.

(2) The category or categories of consumers' personal information it has disclosed for a business purpose, or if the business has not disclosed the consumers' personal information for a business purpose, it shall disclose that fact.

(d) A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 4. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.120.

(a) A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least~~between~~ 13 years of age and less that~~and~~[7] 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

(d) A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 5. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.125.

(a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer.

(D) Suggesting that the consumer will receive a different price or rate for goods or services

[7] AB 1355

or a different level or quality of goods or services.

(2) Nothing in this subdivision prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer~~-~~business[8] by the consumer's data.

(b) (1) A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference is directly related to the value provided to the consumer~~-~~business[9] by the consumer's data.

(2) A business that offers any financial incentives pursuant to this subdivision ~~(a),~~ shall notify consumers of the financial incentives pursuant to Section 1798.130~~5~~.[10]

(3) A business may enter a consumer into a financial incentive program only if the consumer gives the business prior opt-in consent pursuant to Section 1798.130~~5~~ that ~~which~~[11] clearly describes the material terms of the financial incentive program, and which may be revoked by the consumer at any time.

(4) A business shall not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 6. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.130.

(a) In order to comply with Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115~~, and if the~~ business ~~maintains an Internet Web site, a Web site address.~~[12]
(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.[13]

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business's ~~s~~ duty to disclose and deliver the information within 45 days of receipt

[8] AB 1355
[9] AB 1355
[10] AB 1355
[11] AB 1355
[12] AB 1564; slight AB 25 edits superseded here by AB 1564
[13] AB 1564

of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business's ~~s~~ receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but[14] shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.[15]

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers'

[14] AB 25
[15] AB 25

privacy rights, or if the business does not maintain those policies, on its internet website, ~~Internet Web site~~,[16] and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105,[17] 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business's ~~s~~ privacy practices or the business's ~~s~~ compliance with this title are informed of all requirements in Sections 1798.100, 1798.105,[18] 1798.110, 1798.115, 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business's ~~s~~ verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 7. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.135.

(a) A business that is required to comply with Section 1798.120 shall, in a form that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A

[16] AB 25
[17] AB 1355
[18] AB 1355

business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.140.

For purposes of this title:

(a) "**Aggregate consumer information**" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.

(b) "**Biometric information**" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or

rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "**Business**" means:

(1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners~~,~~ that collects consumers' personal information~~,~~ or on the behalf of which ~~such~~ that[19] information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:

(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.

(B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.

(C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

(2) Any entity that controls or is controlled by a business~~,~~ as defined in paragraph (1)~~,~~ and that shares common branding with the business. "Control" or "controlled" means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, servicemark, or trademark.

(d) "**Business purpose**" means the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the operational purpose for which the personal information was collected or processed or for another operational purpose that is compatible with the context in which the personal information was collected. Business purposes are:

(1) Auditing related to a current interaction with the consumer and concurrent transactions, including, but not limited to, counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

(2) Detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity.

(3) Debugging to identify and repair errors that impair existing intended functionality.

(4) Short-term, transient use, provided that[20] the personal information ~~that~~ is not disclosed to another third party and is not used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

[19] AB 1355
[20] AB 1355

(5) Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing advertising or marketing services, providing analytic services, or providing similar services on behalf of the business or service provider.

(6) Undertaking internal research for technological development and demonstration.

(7) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "**Collects**," "**collected**," or "**collection**" means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.

(f) "**Commercial purposes**" means to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction. "**Commercial purposes**" do not include for the purpose of engaging in speech that state or federal courts have recognized as noncommercial speech, including political speech and journalism.

(g) "**Consumer**" means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.

(h) "**Deidentified**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(2) Has implemented business processes that specifically prohibit reidentification of the information.

(3) Has implemented business processes to prevent inadvertent release of deidentified information.

(4) Makes no attempt to reidentify the information.

(i) "**Designated methods for submitting requests**" means a mailing address, email address, i~~I~~nternet ~~W~~web page, ~~I~~internet ~~W~~web[21] portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under this title, and any new, consumer-friendly means of contacting a business, as approved by the Attorney General pursuant to Section 1798.185.

(j) "**Device**" means any physical object that is capable of connecting to the i~~I~~nternet, directly or indirectly, or to another device.

(k) "**Health insurance information**"[22] means a consumer's insurance policy number or subscriber

[21] AB 874; AB 1355

[22] Defined term never used?

identification number, any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is linked or reasonably linkable to a consumer or household, including via a device, by a business or service provider.

(l) "**Homepage**" means the introductory page of an ~~I~~internet ~~W~~web site and any ~~I~~internet ~~W~~web[23] page where personal information is collected. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, a link within the application, such as from the application configuration, "About," "Information," or settings page, and any other location that allows consumers to review the notice required by subdivision (a) of Section 1798.13~~4~~5,[24] including, but not limited to, before downloading the application.

(m) "**Infer**" or "**inference**" means the derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data.

(n) "**Person**" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.[25]

(o) (1) "**Personal information**" means information that identifies, relates to, describes, is reasonably[26] capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably[27] capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, i~~I~~nternet p~~P~~rotocol[28] address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an i~~I~~nternet ~~W~~web[29] site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

---

[23] AB 1355
[24] AB 1355
[25] AB 1355
[26] AB 874
[27] AB 874
[28] AB 874; AB 1355
[29] AB 874; AB 1355

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. ~~section~~ [30]1232g; ~~,~~ 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(2) "**Personal information**" does not include publicly available information. For ~~these~~ purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records~~, if any conditions associated with such information~~. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. ~~Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include~~ consumer ~~information that is deidentified or aggregate~~ consumer ~~information.~~[31]

(3) "**Personal information**" does not include consumer information that is deidentified or aggregate consumer information.[32]

(p) "**Probabilistic identifier**" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories enumerated in the definition of personal information.

(q) "**Processing**" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means.

(r) "**Pseudonymize**" or "**Pseudonymization**" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(s) "**Research**" means scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a business's service or device for other purposes shall be:

(1) Compatible with the business purpose for which the personal information was collected.

(2) Subsequently pseudonymized and deidentified, or deidentified and in the aggregate, such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer.

(3) Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

(4) Subject to business processes that specifically prohibit reidentification of the information.

---

[30] AB 1355
[31] AB 874; minor edit in AB 1355 likely superseded by AB 874 strikeout
[32] AB 874

(5) Made subject to business processes to prevent inadvertent release of deidentified information.

(6) Protected from any reidentification attempts.

(7) Used solely for research purposes that are compatible with the context in which the personal information was collected.

(8) Not be used for any commercial purpose.

(9) Subjected by the business conducting the research to additional security controls that[33] limit access to the research data to only those individuals in a business as are necessary to carry out the research purpose.

(t) (1) "**Sell**," "**selling**," "**sale**," or "**sold**," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.

(2) For purposes of this title, a business does not sell personal information when:

(A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:

(i) The business has provided notice of that information is[34] being used or shared in its terms and conditions consistent with Section 1798.135.

(ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose.

(D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with Sections 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with Section 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner

[33] AB 874
[34] AB 874

that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7 of the Business and Professions Code).

(u) "**Service**" or "**services**" means work, labor, and services, including services furnished in connection with the sale or repair of goods.

(v) "**Service provider**" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

(w) "**Third party**" means a person who is not any of the following:

(1) The business that collects personal information from consumers under this title.

(2) (A) A person to whom the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract:

(i) Prohibits the person receiving the personal information from:

(I) Selling the personal information.

(II) Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.

(III) Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

(ii) Includes a certification made by the person receiving the personal information that the person understands the restrictions in subparagraph (A) and will comply with them.

(B) A person covered by this paragraph that violates any of the restrictions set forth in this title shall be liable for the violations. A business that discloses personal information to a person covered by this paragraph in compliance with this paragraph shall not be liable under this title if the person receiving the personal information uses it in violation of the restrictions set forth in this title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the person intends to commit such a violation.

(x) "**Unique identifier**" or "**Unique personal identifier**" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device. For purposes of this subdivision, "family" means a custodial parent or guardian and any minor children over which the parent or guardian has custody.

(y) "**Verifiable consumer request**" means a request that is made by a consumer, by a consumer on

behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information. A business is not obligated to provide information to the consumer pursuant to Sections 1798.100, 1798.105,[35] 1798.110 and 1798.115 if the business cannot verify, pursuant to[36] this subdivision and regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185, that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on such consumer's behalf.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 9. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.145.

(a) The obligations imposed on businesses by this title shall not restrict a business's ~~s~~ ability to:

(1) Comply with federal, state, or local laws.

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(3) Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law.

(4) Exercise or defend legal claims.

(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.

(6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing, including on a device, personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California.

(b) The obligations imposed on businesses by Sections 1798.110 to 1798.135, inclusive, shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law and shall not prevent a business from providing the personal information of a consumer to a person covered by an evidentiary privilege under California law as part of a privileged communication.

(c) (1) This title shall not apply to any of the following:

(A) Medical information governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or protected health information that is

[35] AB 1355
[36] AB 874

collected by a covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5).

(B) A provider of health care governed by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) or a covered entity governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph (A) of this section.

(C) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects, also known as the Common Rule, pursuant to good clinical practice guidelines issued by the International Council for Harmonisation or pursuant to human subject protection requirements of the United States Food and Drug Administration.

(2) For purposes of this subdivision, the definitions of "medical information" and "provider of health care" in Section 56.05 shall apply and the definitions of "business associate," "covered entity," and "protected health information" in Section 160.103 of Title 45 of the Code of Federal Regulations shall apply.

(d) (1) This title shall not apply to an activity involving the collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by ~~the~~ sale ~~of~~ personal information ~~to or from~~ a consumer reporting agency, as defined in subdivision (f) of Section 1681a of Title 15 of the United States Code, by a furnisher of information, as set forth in Section 1681s-2 of Title 15 of the United States Code, who provides information for use in a consumer report, as defined in ~~if that information is to be reported in, or used to generate, a~~ consumer ~~report as defined by~~ subdivision (d) of Section 1681a of Title 15 of the United States Code, and by a user of a consumer report as set forth in Section 1681b of Title 15 of the United States Code~~use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.)~~.[37]

(2) Paragraph (1) shall apply only to the extent that such activity involving the collection, maintenance, disclosure, sale, communication, or use of such information by that agency, furnisher, or user is subject to regulation under the Fair Credit Reporting Act, section 1681 et seq., Title 15 of the United States Code and the information is not used, communicated, disclosed, or sold except as authorized by the Fair Credit Reporting Act.[38]

(3) This subdivision shall not apply to Section 1798.150.[39]

(e) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of

[37] AB 1355
[38] AB 1355
[39] AB 1355

the Financial Code). This subdivision shall not apply to Section 1798.150.

(f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S 2721 et seq.). This subdivision shall not apply to Section 1798.150.

(g) [40](1) Section 1798.120 shall not apply to vehicle information or ownership information retained or shared between a new motor vehicle dealer, as defined in Section 426 of the Vehicle Code, and the vehicle's manufacturer, as defined in Section 672 of the Vehicle Code, if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to Sections 30118 to 30120, inclusive, of Title 49 of the United States Code, provided that the new motor vehicle dealer or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose.

(2) For purposes of this subdivision:

(A) "Vehicle information" means the vehicle information number, make, model, year, and odometer reading.

(B) "Ownership information" means the name or names of the registered owner or owners and the contact information for the owner or owners.

(h) [41] (1) This title shall not apply to any of the following:

(A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.

(B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

(C) Personal information that is necessary for the business to retain to administer benefits for another natural person relating to the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of administering those benefits.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

---

[40] This Section (g) added by AB 1146
[41] This Section (h) added by AB 25

(C) "Medical staff member" means a licensed physician and surgeon, dentist, or podiatrist, licensed pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code and a clinical psychologist as defined in Section 1316.5 of the Health and Safety Code.

(D) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(E) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall not apply to subdivision (b) of Section 1798.100 or Section 1798.150.

(4) This subdivision shall become inoperative on January 1, 2021.

~~(g)~~(i) Notwithstanding a business'~~s~~ obligations to respond to and honor consumer rights requests pursuant to this title:

(1) A time period for a business to respond to any verified consumer request may be extended by up to 90 additional days where necessary, taking into account the complexity and number of the requests. The business shall inform the consumer of any such extension within 45 days of receipt of the request, together with the reasons for the delay.

(2) If the business does not take action on the request of the consumer, the business shall inform the consumer, without delay and at the latest within the time period permitted of response by this section, of the reasons for not taking action and any rights the consumer may have to appeal the decision to the business.

(3) If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

~~(h)~~(j) A business that discloses personal information to a service provider shall not be liable under this title if the service provider receiving the personal information uses it in violation of the restrictions set forth in the title, provided that, at the time of disclosing the personal information, the business does not have actual knowledge, or reason to believe, that the service provider intends to commit such a violation. A service provider shall likewise not be liable under this title for the obligations of a business for which it provides services as set forth in this title.

~~(i)~~(k) This title shall not be construed to require a business to collect personal information that it would not otherwise collect in the ordinary course of its business, retain personal information for longer than it would otherwise retain such information in the ordinary course of its business, or[42] reidentify or otherwise link information that is not maintained in a manner that would be considered personal information.

[42] AB 1355

~~(j)~~(l) The rights afforded to consumers and the obligations imposed on the business in this title shall not adversely affect the rights and freedoms of other consumers.

~~(k)~~(m) The rights afforded to consumers and the obligations imposed on any business under this title shall not apply to the extent that they infringe on the noncommercial activities of a person or entity described in subdivision (b) of Section 2 of Article I of the California Constitution.

~~(l)~~(n) (1)[43] The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135 shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit or government agency.

(2) For purposes of this subdivision:

(A) "Contractor" means a natural person who provides any service to a business pursuant to a written contract.

(B) "Director" means a natural person designated in the articles of incorporation as such or elected by the incorporators and natural persons designated, elected, or appointed by any other name or title to act as directors, and their successors.

(C) "Officer" means a natural person elected or appointed by the board of directors to manage the daily operations of a corporation, such as a chief executive officer, president, secretary, or treasurer.

(D) "Owner" means a natural person who meets one of the following:

(i) Has ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business.

(ii) Has control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

(iii) Has the power to exercise a controlling influence over the management of a company.

(3) This subdivision shall become inoperative on January 1, 2021

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 10. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.150.

(a) (1) Any consumer whose nonencrypted ~~or~~ and[44] nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not

[43] This section (n) added by AB 1355
[44] AB 1355

greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

(c) The cause of action established by this section shall apply only to violations as defined in subdivision (a) and shall not be based on violations of any other section of this title. Nothing in this title shall be interpreted to serve as the basis for a private right of action under any other law. This shall not be construed to relieve any party from any duties or obligations imposed under other law or the United States or California Constitution.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 11. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.155.

(a) Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent

to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 12. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.160.

(a) A special fund to be known as the "Consumer Privacy Fund" is hereby created within the General Fund in the State Treasury, and is available upon appropriation by the Legislature to offset any costs incurred by the state courts in connection with actions brought to enforce this title and any costs incurred by the Attorney General in carrying out the Attorney General's duties under this title.

(b) Funds transferred to the Consumer Privacy Fund shall be used exclusively to offset any costs incurred by the state courts and the Attorney General in connection with this title. These funds shall not be subject to appropriation or transfer by the Legislature for any other purpose, unless the Director of Finance determines that the funds are in excess of the funding needed to fully offset the costs incurred by the state courts and the Attorney General in connection with this title, in which case the Legislature may appropriate excess funds for other purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.175.

This title is intended to further the constitutional right of privacy and to supplement existing laws relating to consumers' personal information, including, but not limited to, Chapter 22 (commencing with Section 22575) of Division 8 of the Business and Professions Code and Title 1.81 (commencing with Section 1798.80). The provisions of this title are not limited to information collected electronically or over the Internet, but apply to the collection and sale of all personal information collected by a business from consumers. Wherever possible, law relating to consumers' personal information should be construed to harmonize with the provisions of this title, but in the event of a conflict between other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.180.

This title is a matter of statewide concern and supersedes and preempts all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection and sale of consumers' personal information by a business.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative September 23, 2018, pursuant to Section 1798.199.)

1798.185.

(a) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to, the following areas:

(1) Updating as needed additional categories of personal information to those enumerated in subdivision (c) of Section 1798.130 and subdivision (o) of Section 1798.140 in order to address changes in technology, data collection practices, obstacles to implementation, and privacy concerns.

(2) Updating as needed the definition of unique identifiers to address changes in technology, data collection, obstacles to implementation, and privacy concerns, and additional categories to the definition of designated methods for submitting requests to facilitate a consumer's ability to obtain information from a business pursuant to Section 1798.130.

(3) Establishing any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.

(4) Establishing rules and procedures for the following:

(A) To facilitate and govern the submission of a request by a consumer to opt-out of the sale of personal information pursuant to ~~paragraph (1) of subdivision (a) of~~ Section 1798.120~~45~~.[45]

(B) To govern business compliance with a consumer's opt-out request.

(C) For the development and use of a recognizable and uniform opt-out logo or button by all businesses to promote consumer awareness of the opportunity to opt-out of the sale of personal information.

(5) Adjusting the monetary threshold in subparagraph (A) of paragraph (1) of subdivision (c) of Section 1798.140 in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(6) Establishing rules, procedures, and any exceptions necessary to ensure that the notices and information that businesses are required to provide pursuant to this title are provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer, including establishing rules and guidelines regarding financial incentive offerings, within one year of passage of this title and as needed thereafter.

(7) Establishing rules and procedures to further the purposes of Sections 1798.110 and 1798.115 and to facilitate a consumer's or the consumer's authorized agent's ability to obtain information pursuant to Section 1798.130, with the goal of minimizing the administrative burden on consumers, taking into account available technology, security concerns, and the burden on the business, to govern a business's determination that a request for information received ~~by~~ from[46] a consumer is a verifiable consumer request, including treating a request submitted through a password-protected account maintained by the consumer with the business while the consumer is logged into the account as a verifiable consumer request and providing a mechanism for a consumer who does not maintain an account with the business to request information through the business's authentication of the consumer's identity, within one year of passage of this title and as needed thereafter.

(b) The Attorney General may adopt additional regulations as ~~necessary to further the purposes of this title.~~follows:[47]

(1) To establish rules and procedures on how to process and comply with verifiable consumer requests for specific pieces of personal information relating to a household in order to address obstacles to implementation and privacy concerns.

(2) As necessary to further the purposes of this title.

[45] AB 1355
[46] AB 1355
[47] AB 1355

(c) The Attorney General shall not bring an enforcement action under this title until six months after the publication of the final regulations issued pursuant to this section or July 1, 2020, whichever is sooner.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 13. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.190.

If a series of steps or transactions were component parts of a single transaction intended from the beginning to be taken with the intention of avoiding the reach of this title, including the disclosure of information by a business to a third party in order to avoid the definition of sell, a court shall disregard the intermediate steps or transactions for purposes of effectuating the purposes of this title.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.192.

Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable. This section shall not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale of the consumer's personal information, or authorizing a business to sell the consumer's personal information after previously opting out.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 14. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.194.

This title shall be liberally construed to effectuate its purposes.

(Added by Stats. 2018, Ch. 55, Sec. 3. (AB 375) Effective January 1, 2019. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.196.

This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 15. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

1798.198.

(a) Subject to limitation provided in subdivision (b), and in Section 1798.199, this title shall be operative January 1, 2020.

(b) This title shall become operative only if initiative measure No. 17-0039, The Consumer Right to Privacy Act of 2018, is withdrawn from the ballot pursuant to Section 9604 of the Elections Code.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 16. (SB 1121) Effective September 23, 2018.)

1798.199.

Notwithstanding Section 1798.198, Section 1798.180 shall be operative on the effective date of the act adding this section.

(Added by Stats. 2018, Ch. 735, Sec. 17. (SB 1121) Effective September 23, 2018. Operative September 23, 2018.)

Implementing the California Consumer Privacy Act (CCPA)

I. What is the CCPA?

The California Consumer Privacy Act ("CCPA"), California Civil Code § 1798.100, *et seq.,* imposes obligations on any **business** that **collects** and/or **processes personal information** about California residents (and meets certain additional criteria). The Governor signed into law a number of amendments to the CCPA on October 11, 2019, and the State Attorney General recently released draft regulations that add a number of new disclosure requirements and regulate the handling of consumer requests, identity verification, special rules regarding minors, and financial incentives.

II. What Type of "Business" is Subject to the CCPA?

Any business that collects personal information should be concerned about the CCPA. The term "business" is broad and includes: "a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners[.]"[1]

Subject to certain limited exceptions, the CCPA applies to businesses that meet any of the following criteria:

- annual gross revenues in excess of **$25M**;
- alone or in combination, annually buy, receive for the business's commercial purposes, sell, or share for commercial purposes, alone or in combination, the personal information of **50,000 or more California residents, households, or devices**; or
- derive **50% or more of annual revenues** from selling consumers' personal information.

The CCPA also applies to an entity that controls or is controlled by such a business and shares common branding with the business.

III. What Does "Collecting" or "Processing" Personal Information Mean?

- **Collecting** "means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[2]

[1] Cal. Civ. Code § 1798.140(c)(1).
[2] *Id*. at § 1798.140(e).

- **Processing** "means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means."[3]
- **Service Providers** are subject to CCPA but are not responsible for the obligations of their business customers, provided that they are contractually restricted from using the personal information they process only to perform the contracted services.[4]

IV. What is "Personal Information"?

Personal Information under the CCPA means "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[5]

Personal Information specifically includes, but is not limited to, the following:

- Identifiers such as:

  ◘ Name ◘ Alias ◘ Postal Address ◘ Unique Personal Identifier ◘ Online Identifier ◘ IP Address ◘ Email ◘ Account Name ◘ Social Security Number ◘ Driver's License Number ◘ Passport Number, or other similar identifiers.

- Categories of Personal Information identified by California's Customer Records Law,[6] such as:

  ◘ Signature ◘ Physical Characteristics or Description ◘ Telephone Number ◘ Passport Number ◘ Driver's License or State ID Card Number ◘ Insurance Policy Number ◘ Education ◘ Employment ◘ Employment History ◘ Bank Account Number ◘ Credit Card Number ◘ Debit Card Number, or any other financial information, medical information, or health insurance information;

- Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- Biometric information;
- Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement;
- Geolocation data;
- Audio, electronic, visual, thermal, olfactory, or similar information;
- Professional or employment-related information, and education information; and

---

[3] *Id*. at § 1798.140(q).
[4] *Id*. at § 1798.145(h).
[5] *Id*. at § 1798.140(o).
[6] *Id*. at § 1798.80(e).

- Inferences drawn from any of the information identified above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

V. What Rights do Consumers Have Under the CCPA?

- Right to know what personal information is collected, sold, and disclosed (and to whom), and to receive a copy of the specific information the business has about him or her.
- Right to opt-out of the "sale" of personal information.
- Right to deletion.
- Right to equal service and price, even if consumer exercises any rights under the CCPA.
- Right to use an authorized agent to exercise CCPA rights.

VI. What Does the CCPA Require?

Subject to certain exceptions and conditions, businesses subject to the CCPA are required to:

- Make additional disclosures before collection identifying what personal information is collected, from what sources, for what purpose, with whom it will be shared, the consumer's rights under the CCPA and other related information.
- Respond to a consumer's verified request on a short time line (acknowledge receipt within 10 days and substantively respond, generally, within 45 days of receipt).
- Upon consumer demand, delete the consumer's personal information held by the company or its service providers (a number of important exceptions exist to retain such information).
- Upon consumer demand, exclude the consumer from all data sharing for commercial purposes.
- Provide a "Do Not Sell My Personal Information" link on the business homepage and in the privacy policy.

There are exceptions in the CCPA for certain types of data already subject to state and federal privacy restrictions, but in certain cases (e.g., GLBA and DPPA) the exception is only to the extent the laws are applicable and are in conflict with the CCPA.

VII. Does the CCPA Impact Loyalty Programs or Customer Accounts?

The CCPA prohibits, among other activities, denying, offering a different level of quality, or suggesting a consumer would receive a different level of quality, of goods or services when exercising rights under the CCPA. A business cannot require consumers to create an account in order to exercise their rights.

However, there are key exceptions:

1. A business may charge a different price or offer a different level of quality of goods or services when that difference is "reasonably related" to the value provided to the business

by the consumer's own data. In that case, the business must disclose a good faith estimate of the value of the consumer's data.[7]

2. A business may also offer financial incentives or offer different prices, rates, levels or quality of goods and services as compensation for the collection of personal information, but only when that activity is "directly related" to the value provided.

This language raises questions about whether and to what extent the CCPA restricts common loyalty programs and customer account practices. Recent amendments by the Attorney General have only complicated this issue.

VIII. How Can the Holland & Knight Team Help?

- Counsel on the applicability and scope of the CCPA and other California-specific consumer protection laws, particularly how they impact business operations and legal compliance.
- Develop CCPA policies, procedures, training and supplement enterprise changes within business units and information systems impacted by the CCPA.
- Develop information governance strategy for a business's personal information repositories and related data systems. In addition to addressing CCPA, these efforts can be leveraged for a broader array of current and forthcoming federal, state and foreign laws and regulations on privacy and cybersecurity (e.g., pending U.S. legislation, GDPR, PIPEDA).
- Global or national privacy program assessments and counseling (recommendations and remediation).
- Provide strategic advice with respect to: (1) loyalty programs (2) facilitating data subject rights and requests; (3) online behavioral advertising; and (4) data sharing and monetization practices.
- Advise on CCPA with respect to vendor and commercial customer contracts.
- Counsel on developments in CCPA amendments, AG regulations and guidance, and enforcement, potentially in connection with broader advice on pending federal and state legislation.
- Develop incident response plans and breach notification policies.
- Help tackle the agenda and to-do list below.

IX. CCPA: Your Agenda and To-Do List

A. Corporate entities

(1) Identify all entities subject to CCPA within the business

[7] Reg. § 999.307(b)(5).

(2) Determine which entities are “affiliates” (common control and common branding)

B. Data Mapping

(1) Identify all internal systems with consumer Personal Information (“PI”)

(2) Identify all accessible cloud systems with consumer PI

(3) Identify all vendor systems and other third party recipients of consumer PI, and determine if the vendor is a “service provider” (e.g., restricted use of PI) or a “third party” (including manual sharing, automated sharing, web front sharing)

(4) Identify all data flows from websites and mobile apps, including cookies and tags

(5) Identify scope of consumers (e.g., not businesses, presence of minors)

(6) Exclude data, if any, not subject to CCPA (e.g., HIPAA, GLBA)

(7) Evaluate all business use cases for PI

(8) Document/chart all data repositories, all vendors, and all data elements

C. Data Subject Rights

(1) Develop consumer and residency verification process:

(a) Consumer account login

(b) Name + email with verification by email link/passcode

(c) Other?

(2) Document plan for disclosure requests: What data will be disclosed, and why or why not

(3) Document plan for deletion requests: What data will be deleted, and why or why not (e.g., exceptions)

(4) Document plan for do not sell requests: What outbound data will be blocked

(5) Implement systems and procedures to respond to requests (e.g., procedures, ticketing systems, consumer portal, system APIs); use of vendor solutions

(a) Two means of submission

(b) 45/90 day deadline

(6) Implement systems and procedures to block data sharing for consumers who issue a do not sell request (internal block lists; cookie controls)

(7) Implement process to notify vendors of requests, if and where necessary

(8) Implement escalation path for complaints and issues

(9) Assign internal resources to manage DSR requests on a going forward basis

(a) DSR workflow and process

(b) Call center staffing/training

D. Policies and Contracts

(1) Update online privacy policy (disclosure of various categories; consumer rights requests)

(2) Address opt-in for minors under 13 and 13-16, if applicable

(3) Review/update vendor contracts as necessary, and going forward

(4) Update CA employee privacy notice

(5) Privacy policy for physical CA locations

(6) Review loyalty and promotions programs, verify no potential discrimination for assertions of consumer rights

(7) Address "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information"

Practice Profile

Our Data Strategy, Security & Privacy Team helps clients capitalize on data and tech capabilities while managing associated risks and incidents that arise. We have advised and represented clients on many of the largest public (and nonpublic) data issues and security incidents in the U.S.

We deliver: 1) pragmatic business-oriented solutions to address legal needs, 2) documentation you need for legal compliance and contracting, and 3) strategic representation during an incident, as well as in investigations and litigations that may follow. We do it efficiently, with transparent budgeting and billing.

How To Reach Us

Paul Bond	**Mark H. Francis**	**Mark S. Melodia**	**Ashley L. Shively**
Partner, Philadelphia	Partner, New York	Partner, New York	Partner, San Francisco
215.252.9535	212.513.3572	212.513.3583	415.743.6906
Paul.Bond@hklaw.com	Mark.Francis@hklaw.com	Mark.Melodia@hklaw.com	Ashley.Shively@hklaw.com

< https://www.hklaw.com/en/services/practices/technology-and-cybersecurity/data-strategy-security-and-privacy >

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer's ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms' Data* (Aug. 3, 2017), https://www.cio.com (explaining that "[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.")' *See also Criminal-Seeking-Hacker' Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Securing Communication of Protected Client Information").

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,[6] and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.[7]

---

[6] The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

[7] In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g.*, *Cybersecurity Resources*, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[8] The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. (Emphasis added.)[9]

In recommending the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to 'keep abreast of changes in the law and its practice.' The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [10]

---

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[10] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[11]

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

---

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).
[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").
[14] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF'L CONDUCT R. 1.15 (2018).
[15] *See also* MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2018).
[16] The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); *See also* National Cyber Security Centre "Ten Steps to Cyber Security" [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.[18] The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. "One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents."[19] While every lawyer's response plan should be tailored to the lawyer's or the law firm's specific practice, as a general matter incident response plans share common features:

> The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

[18] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting "an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.").

[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.[20]

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[21] These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

[21] We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).[22] Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[23] The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[24]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

---

[22] The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

[24] *Id.* at (c).

- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[25]

As this Committee recognized in ABA Formal Opinion 477R:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.[26] Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.[27] As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[28]

---

[25] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2018). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

[26] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

[27] MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. [18] (2018) ("The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.")

[28] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.[29] In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.[30] We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.[31]

---

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[30] This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

[31] Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: "If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach."[32] The Committee advised:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).[33]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.[34]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

---

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[33] *Id.*

[34] MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property." Funds must be kept in a separate account, and "[o]ther property shall be identified as such and appropriately safeguarded." Model Rule 1.15(a) also provides that, "Complete records of such account funds and other property shall be kept by the lawyer . . . ." Comment [1] to Model Rule 1.15 states:

> A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form. Comment [1] uses as examples "securities" and "property" that should be kept separate from the lawyer's "business and personal property." That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15's safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, "Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information."

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client."[35] When electronic "information relating to the representation" of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the former client. Rule 1.9(c) provides that a lawyer "shall not . . . reveal" the former client's information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] We also note that Rule 1.16(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.[38] Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

---

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).
[36] *See* Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent's argument that the court should engraft an additional element of proof in a disciplinary charge because "such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.").
[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).
[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.[39]

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

[39] *Cf.* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.[40] Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

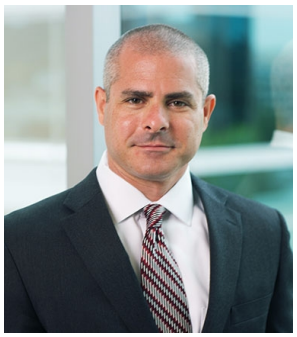
III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] *Id.*
[43] *Id.*
[44] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.
[45] Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

NEWMEYER DILLION



JOSHUA BEVITZ

Partner

Joshua Bevitz

Partner
joshua.bevitz@ndlf.com

Walnut Creek, CA
925-988-3226

Publications

Companies: Per the American Bar Association, Here are Your Attorneys' Obligations Related to Cyberattacks

October 26, 2018 – Published Article

By Joshua Bevitz

As cyberattacks begin to become more and more frequent, the American Bar Association ("ABA") continues to issue opinions regarding the ethical duties of attorneys in relation to them. On October 17, 2018, the ABA issued yet another, Formal Opinion 483.

Formal Opinion 483 allows companies to better understand their attorneys' obligations to guard against cyberattacks, to protect the electronic information provided to them, and to respond if an attack occurs. An attorney's failure to adhere to these guidelines could result in damage to your business.

I. Attorneys have an ethical duty to protect their clients against cyberattacks.

Model Rule 1.1 states: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment 8 to Rule 1.1 reads, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (Emphasis added.)

As it relates to cyberattacks, Formal Opinion 483 specifies, "Lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." That is, as with paper files, lawyers have the same obligation to ensure the security of electronic files.

However, a successful cyberattack does not necessarily mean an attorney has committed an ethical violation. Rather, an ethical violation only results if the attorney did not take reasonable steps to protect its electronic files.

II. Attorneys have ethical duties to address cyberattacks through proactive incident response plans, investigations, and proper notifications.

Incident Response Plan.

When a cyberattack is successful, Model Rule 1.1 requires an attorney to stop the attack and mitigate the damage. As such, the ABA recommends that attorneys have a preexisting incident response plan in place with specific plans and procedures for responding so that any damage and disruption resulting from the attack can be minimized.

The incident response plan should also outline who has been tasked with carrying out each step in addition to who is assigned the overall duty to ensure that the incident response plan is undertaken. Moreover, Formal Opinion 483

specifically states that “a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer’s clients.”

Investigation.

Formal Opinion 483 also specifies that a competent attorney must make reasonable attempts to make sure the attack has been stopped and to determine what happened, including whether data was lost or accessed. The investigation should yield sufficient information so that the attorney can make accurate disclosures to his clients that are consistent with the ethical duties of honesty and communication.

Notification to Current Clients – Depending on the Breach.

Formal Opinion 483 states that cyberattack notification requirements “will depend on the type of breach that occurs and the nature of the data compromised by the breach.” Notification to the client is required if material client information has actually “been accessed, disclosed or lost in a breach” or if it reasonable to suspect as much. The notification should be sufficient for attorney’s clients to make informed decisions regarding the next steps to take.

An attorney should also notify clients that reasonable steps were taken to determine exactly what information was affected and advise them of a plan to deal with it, such as potentially trying to recover lost information or taking steps to fortify cybersecurity. Formal Opinion 483 also concludes that an attorney must reasonably keep his clients apprised regarding post-attack developments.[1]

Law Firms - Per The ABA, Take The Following Actions To Protect Your Current and Former Clients and Yourselves.

Current Clients

Cyberattacks on law offices will only increase in frequency given the sensitive and potentially valuable information in electronic client files. Attorneys should take reasonable actions to do all of the following:

1. Protect your computer system and ensure your vendors are doing the same;
2. Have an incident response plan in place to stop the attack and minimize the damage;
3. Conduct an investigation to determine exactly what happened; and
4. Notify and advise clients as required.

Former Clients

Formal Opinion 483 treats former clients differently because the Model Rules do not address an attorney’s duty to notify a former client of a cyberattack.[2] The Committee did note that, pursuant to Rule 1.16(d), attorneys should avoid retaining client files indefinitely.

As such, Formal Opinion 483 recommends that attorneys reach agreements with clients at the end of representation regarding how electronic files will be handled. Absent agreements, the Committee recommends that attorneys follow an electronic document retention schedule to reduce the amount of client information they retain. Following those recommendations could reduce the chance of legal exposure if a successful cyberattack in fact occurs.

Failure to adhere to these guidelines could result in damage to your current and former clients. It could also lead to your own civil liability and land you in ethical hot water.

---

[1] Importantly, an attorney has legal duties separate from ethical duties. As such, if personally identifiable information of a client is affected, an attorney should comply with any applicable privacy laws and other statutes, including as to their notification requirements.

[2] Again, even though an attorney may not have an ethical duty to notify a former client of cyberattack, an attorney should still comply with notification requirements pursuant to any applicable privacy laws and other statutes.

Featured

July 2019 **Joshua Bevitz**

Five Ways Law Firms Can Protect Themselves from the Consequences of Cyberattacks

The frequency of cyberattacks on law offices will likely increase because of the confidential and valuable data that attorneys store in electronic client files. In conjunction with the American Bar Association's ("ABA") Formal Opinion 483, this article details five proactive steps law firms should take.

ABA Formal Opinion 483 clarifies attorneys' obligations to prepare for cyberattacks, to safeguard information provided to them, and to respond appropriately if an attack occurs. Formal Opinion 483 states: "Lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data." In other words, attorneys must secure their electronic files. While ABA rules are not technically binding on attorneys, states will likely issue similar rules, and practitioners should be prepared to follow these regulations.

1. Ensure Reasonable Computer Protection Systems Are In Place

Model Rule 1.1 states: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Comment 8 to Rule 1.1 reads, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

Every law firm should have current technology protecting its computer systems, including office resources connected to the internet, and as well as external data sources. A firm's IT department should perform periodic, regular reviews to determine whether additional protections are warranted and whether the current security system is "reasonable." In addition, the IT department should monitor whether patching existing protections is necessary based on newly developed cyberattacks. At least one technically-competent partner should be assigned as the liaison to the IT department to ensure its responsibilities are being met. If a law firm does not have an IT department, an outside cybersecurity firm should be consulted and retained.

1. Train and Test Your Attorneys and Staff
   Most successful cyberattacks are the result of human error and not a frontal breach of a computer system. In other words, a user gets tricked into clicking a link that results in a virus or other attacking agent obtaining access to the system. As a result, all users should be regularly trained regarding what types of cyberattack vectors exist, and what attackers try to do to trick users. However, law firms should take matters a step further and conduct fake phishing campaigns to test their employees. Numerous third-party cyber companies can provide this service if a firm does not have internal resources to do so. Trial by error is often the best way to learn.
2. Ensure Third Party Vendors Have Reasonable Cyber Protection Systems in Place
   Importantly, law firms should ensure that external vendors have reasonable security protections in place to protect the data provided to them. If a vendor does not have reasonable protections, the vendor must be required to implement such protections immediately or the firm should retain another vendor that does provide such protection. Law firms can be held responsible to their clients if they do ensure vendor security exists. One proven approach for law firms is contractually require vendors to adhere to a specific cybersecurity framework and to provide the law firm the right t audit them.

3. Limit the Amount of Time Client Files Are Retained
   The longer a law firm retains its electronic files, the longer those files are susceptible to being attacked. Every law firm should have a written document retention policy, which should be followed and monitored, that applies to both hard and electronic copies of files and documents. The amount of time client files are retained after the conclusion of a matter should be limited as agreed to as part of the initial engagement agreement.
4. Know How to Respond
   Law firms should have a plan in place to deal with cyberattacks when they happen. Having an effective, comprehensive plan will allow a firm to halt the attack and minimize any damage and disruption as soon as possible after the attack becomes known. The plan should specify each step that takes place and who is responsible for taking it. High-level partners should be assigned to the response team to provide leadership and permit executive decision making to occur quickly.

One of the key steps in the response plan should include discovering what occurred and whether client data was compromised. This step is vitally important so that law firms can notify clients in a timely fashion, if their data was taken or destroyed. The notification should be sufficiently detailed so that the client can decide what next steps, if any, should be taken as a result of the attack. Law firms should also make sure they notify clients of any efforts to recover data and what additional protections, if any, are being put into place.

Failing to take the five steps outlined above could not only result in the breach of an attorney's ethical duties, but it could also lead to civil liability. Law firms must proactively protect themselves and their clients' confidential data from cyberattacks.

Joshua Bevitz

Joshua Bevitz is a partner in Newmeyer & Dillion's Walnut Creek office, and a member of the firm's Privacy & Data Security practice. As an experienced insurance litigator, he advises his clients on proactive measures and potential pitfalls related to their cyber insurance policies. For questions on how you can protect your business, you can reach him at joshua.bevitz@ndlf.com.

Journal of Empirical Legal Studies
Volume 5, Issue 3, 551–591, September 2008

Let's Not Make a Deal: An Empirical Study of Decision Making in Unsuccessful Settlement Negotiations

*Randall L. Kiser, Martin A. Asher, and Blakeley B. McShane**

This study quantitatively evaluates the incidence and magnitude of errors made by attorneys and their clients in unsuccessful settlement negotiations. The primary study analyzes 2,054 contested litigation cases in which the plaintiffs and defendants conducted settlement negotiations, decided to reject the adverse party's settlement proposal, and proceeded to arbitration or trial. The parties' settlement positions are compared with the ultimate award or verdict, revealing a high incidence of decision-making error by both plaintiffs and defendants. This study updates and enhances three prior studies of attorney/litigant decision making, increasing the number of cases in the primary data sets more than threefold, adding 72 explanatory variables from 19 classes, applying a multivariate analysis, presenting an historical review of error rates during the 1964–2004 period, and comparing the primary study error rates with error rates in cases where the parties are represented by attorney-mediators. Notwithstanding these enhancements, the incidence and relative cost of the decision-making errors in this study are generally consistent with the three prior empirical studies, demonstrating the robustness of the earlier works by Samuel Gross and Kent Syverud, and Jeffrey Rachlinski. The multivariate analysis, moreover, shows that the incidence of decision-making error is more significantly affected by "context" variables (e.g., case type and forum) than by "actor" variables (e.g., attorney gender and experience level).

---

*Address correspondence to Randall L. Kaiser, DecisionSet, 550 Hamilton Ave., Ste. 300, Palo Alto, CA 94301; email: rkiser@decisionset.com. Asher is Director, Research and Scholars Programs, Wharton Undergraduate Division, and Adjunct Professor of Finance at The Wharton School, University of Pennsylvania; McShane is a graduate student in the Department of Statistics, The Wharton School, University of Pennsylvania.

We thank Jeffrey Rachlinski, Theodore Eisenberg, and an anonymous review for their insightful comments on previous versions of this article.

I. Introduction

The decision to settle or litigate necessarily requires an assessment of the likely trial outcome.[1] Absent extrinsic motivations, a rational litigant roughly weighs an adversary's settlement proposal against the likely trial outcome, makes some adjustments for attorney fees, court costs, and the possibility of delays and appeals, and either accepts or rejects the adversary's settlement proposal. For litigants unwilling to accept an adversary's settlement offer and intent on obtaining a judgment on the merits, trials are their best alternative to a negotiated agreement (BATNA). As Roger Fisher and William Ury assert in *Getting to Yes*, a party's BATNA "is the standard against which any proposed agreement should be measured. That is the only standard which can protect you both from accepting terms that are too unfavorable and from rejecting terms it would be in your interest to accept."[2]

To test whether attorneys and litigants accurately measure trial outcomes against settlement alternatives in adjudicated cases, this study examines 2,054 California civil cases ultimately resolved through trial or arbitration, following unsuccessful settlement negotiations.[3] The cases were reported in a 38-month period between November 2002 and December 2005; about 20 percent of all California litigation attorneys represented the parties in these cases. The parties' settlement positions in those cases are compared with the ultimate award or verdict to determine whether the parties' probability judgments about trial outcomes were economically

---

[1]Samuel Gross & Kent Syverud, Don't Try: Civil Jury Verdicts in a System Geared To Settlement, 44 UCLA L. Rev. 51 (1996): "Every theory of pretrial bargaining assumes that a negotiated settlement is determined, at least in part, by the parties' predictions of the outcome of the case if it did go to trial."

[2]Rober Fisher & William Ury, Getting to Yes: Negotiating Agreement Without Giving In (Penguin Books 1991).

[3]The vast majority of civil cases, of course, are resolved by voluntary settlements or pretrial proceedings. It is impossible to objectively measure the economic utility of decision making in the settled cases, as the settlement consideration cannot be compared with an actual trial outcome. The results of this study are limited to decision making in adjudicated cases with confirmed settlement positions and, due to this selection bias, may not have any explanatory value in settled cases. As Ward Farnsworth explained in his study of injunctions: "I am not purporting to ask or answer any questions about what happens in cases that settle, so excluding them is just a limitation on what the study means." Ward Farnsworth, Do Parties to Nuisance Cases Bargain After Judgment? A Glimpse Inside the Cathedral, in Behavioral Law & Economics (Cass Sunstein, ed., Cambridge University Press 2000).

efficacious, that is, did the parties commit a decision error by rejecting a settlement alternative that would have been the same as or better than the ultimate award? Employing a multivariate analysis, the study presents a quantitative evaluation of those attorney/client probability judgments regarding liability and damages, the costs of inaccurate probability assessments, and the effect of explanatory variables such as offers of compromise, case type, nature of alleged damages, and forum.

The results of this 38-month study are complemented by a 40-year survey of settlement decisions in adjudicated cases from 1964 to 2004. The 40-year survey indicates whether attorney/litigant decision error rates are constant and whether the incidence of adverse outcomes in the 38-month study is atypical. Lastly, to tentatively assess whether the decision-making errors shown in this study may be attributable to the study attorneys' possible risk-taking propensities and bias against negotiated resolutions, the study results are compared with error rates in cases where the parties are represented by attorney-mediators who meet state-mandated mediator training requirements and have been selected to serve on their local court's panel of mediators. This group of attorney-mediators, skilled in case evaluation and conflict resolution, presumably would exhibit lower decision-making error rates if the study attorneys' error rates resulted from singular risk-taking propensities or anti-settlement biases. Alternatively, similar error rates for the study attorneys and the attorney-mediators could demonstrate that the study attorneys are not uniquely risk seeking or that clients, not their attorneys, assume the dominant role in making settlement decisions.[4]

The study serves two principal purposes. First, it is a large-scale empirical study of settlement decision error in adjudicated cases, demonstrating the extent, costs, and persistence of attorney/litigant judgment error. Second, it updates and evaluates the continued validity of three pioneering empirical studies of attorney/litigant settlement decision making: Samuel Gross and Kent Syverud's 1991 article, "Getting to No: A Study of Settlement Negotiations and the Selection of Cases for Trial," their 1996 study, "Don't

---

[4]Attorneys, of course, are required to abide by "a client's decision whether to accept an offer of settlement of a matter." American Bar Association Model Rules of Professional Conduct, Rule 1.2. In referring to "attorney/litigant" decision making, we intend to convey the collaborative nature of the attorney/client relationship while acknowledging that the client is the ultimate decisionmaker.

Try: Civil Jury Verdicts in a System Geared to Settlement," and Jeffrey Rachlinski's 1996 study, "Gains, Losses and the Psychology of Litigation."[5]

II. A Brief Review of Prior Studies

In the three prior studies by Samuel Gross and Kent Syverud and Jeffrey Rachlinski, the authors analyzed settlement behavior in actual civil cases and concluded that the conventional economics model of rational choice leading to optimal economic outcomes is inapplicable, misleading, or inaccurate. Noting that "the absence of data on pretrial negotiations has handicapped development of this topic," law professors Gross and Syverud first studied a nonrandom sample of 529 cases between June 1985 and June 1986. Their data showed that "the main systemic determinants of success at trial and in pretrial bargaining are contextual and relational [e.g., litigants' resources, reputations, insurance, fee arrangements, repeat litigants]" and that prior theoretical models of attorney/litigant settlement behavior were "quite alien to actual litigation."[6] Specifically, their study challenged a prior theoretical model of litigation posited by George Priest and Benjamin Klein: "the fifty percent implication."[7] According to Priest and Klein's theory, trials occur primarily in "close cases," plaintiffs and defendants are equally adept in predicting trial outcomes, plaintiffs will win about 50 percent of the cases that proceed to trial, and "mistakes" about outcomes will be evenly distributed between plaintiffs and defendants. Priest and Klein's hypotheses, however, are discrepant with the data compiled by Gross and Seyverud:

> Economic theories of trial and pretrial bargaining call to mind the standard image of a competitive market: numerous individuals intelligently pursuing independent self-interests. Social reality, as usual, is inconsiderate of global theories. In this case it provides a competing image that is less susceptible to

---

[5]Samuel Gross & Kent Syverud, Getting to No: A Study of Settlement Negotiations and the Selection of Cases for Trial, 90 Michigan L. Rev. 319 (1991); Gross & Syverud (1996), supra; Jeffrey Rachlinski, Gains, Losses and the Psychology of Litigation 70 S. Cal. L. Rev. 113 (1996).

[6]Gross & Syverud (1991), supra, at 319, 330, 379.

[7]George L. Priest & Benjamin Klein, The Selection of Disputes for Litigation, 13 J. of Legal Studies 1 (1984); George L. Priest, Reexamining the Selection Hypothesis, 14 J. of Legal Studies 215 (1985).

> statistical prediction: stragglers picking their way in the dark, trying to avoid an occasional land mine.[8]

Presaging a broader application of behavioral economics' framing concepts to attorney/litigant settlement behavior, Gross and Syverud observed that plaintiffs usually are more risk averse than defendants; plaintiffs and defendants attach "separate values to each possible outcome"; and "their stakes may be unequal (or equal) with respect to victories, or defeats or both."[9]

In their second study, Gross and Syverud added a sample of 359 cases reported between 1990 and 1991. Their results again conflicted with the Priest-Klein litigation model. Instead of a 50/50 distribution of "mistakes," Gross and Syverud found that plaintiffs were more likely than defendants to make a mistake, that is, to reject a settlement proposal that turned out to be the same as or more favorable than the actual trial award. Plaintiffs were "clear losers" in 61 percent of the cases in their first sample (1985–1986) and in 65 percent of the cases in their second sample (1990–1991). The defendants, in contrast, made mistakes in only 25 percent and 26 percent, respectively, of the cases in the two samples.

In the third major empirical study of attorney/litigant decision making in adjudicated cases, Rachlinski compared final settlement offers with jury awards in 656 cases. His data showed decision error by plaintiffs in 56.1 percent of the cases, contrasted with a defendant decision error rate of 23 percent. Although plaintiffs' decision error rate was markedly higher than defendants' decision error rate, the average cost of plaintiffs' decision error was dramatically smaller ($27,687) than defendants' mean cost of error ($354,900). Observing that litigants' decisions are "suboptimal" and "may not comport with rational theories of behavior," Rachlinski found that the "consistently divergent risk preferences between plaintiff and defendant" could be explained by behavioral economics' framing theories.[10] Litigants' "risk preferences depend upon characterizing a decision as a gain or loss" and "vary systematically depending upon whether they are in the role of plaintiff or defendant."[11] Plaintiffs are consistently risk averse, while defen-

---

[8]Gross & Syverud (1991), supra, at 385.

[9]Gross & Syverud (1991), supra, at 319, 381.

[10]Rachlinski, supra, at 114, 118, 120, 142.

[11]Rachlinski, supra, at 119.

dants are risk seeking. Consequently, plaintiffs generally benefited from litigation and "defendants as a class paid heavily for their decision" to litigate: "When settlement negotiations failed, the plaintiffs were unwittingly forced to undertake a risk that, on average, benefited them and cost the defendants dearly."[12]

III. Data and Methods

A. Data Source

The study database consists of 2,054 contested civil litigation cases reported in *Verdict Search California* during the 38-month period between November 2002 and December 2005. *Verdict Search California*, previously titled *California Jury Verdicts Weekly*, is the primary reporting source for judgments and settlements in California, and the reliability of its reports has been confirmed in law review articles and by research studies.[13] Gross and Syverud, for instance, "concluded that the information contained in the journal is reliable and found no systematic bias among the errors by either plaintiff or defendant to misreport the winning party, the size of the award, or the settlement offers."[14] The Rand Corporation also utilized the data reported in *Verdict Search California* to prepare its periodic reports on jury trials and verdicts in major metropolitan areas, including "Trends in Civil Jury Verdicts Since 1985."[15]

Verdict Search California does not report every verdict rendered in California but relies on voluntary submissions from attorneys and solicits reports based on court dockets and trade publications. The information *Verdict Search California* obtains from attorneys, including the parties, attorneys, factual contentions, damages, results, and settlement offers, is compiled in a draft case report. To confirm the contents of the draft case report,

---

[12]Rachlinski, supra, at 160.

[13]Gross & Syverud (1991), supra; Rachlinski, supra; M.A. Peterson & G.L. Priest, The Civil Jury: Trends in Trial and Verdicts, Cook County, Illinois, 1960–1979 (Rand Institute for Civil Justice 1982); M.G. Shanley & M.A. Peterson, Comparative Justice: Civil Jury Verdicts in San Francisco and Cook Counties, 1959–1980 (Rand Institute for Civil Justice 1983).

[14]Rachlinski, supra, at 149 n.133.

[15]Erik Moller, Trends in Civil Jury Verdicts Since 1985 (Institute for Civil Justice, RAND 1996).

Verdict Search California then attempts to contact counsel for all parties by facsimile and telephone. All information received from the parties' attorneys, *Verdict Search California* affirms, is incorporated in the case report. Verdict Search publishes similar weekly verdict reports for the courts of New York and Texas and monthly reports for four other state courts.

Cases reported in *Verdict Search California* during the 38-month study period were included in the study database if they met five basic requirements: (1) a jury verdict, judge's decision, or arbitrator's award was entered in a specific monetary amount; (2) the plaintiff submitted a settlement demand in a specific monetary amount; (3) the defendant made a settlement offer in a specific monetary amount or its settlement offer was described as "none"; (4) there was no reported disagreement among the parties regarding the amount of the ultimate result and the parties' prior settlement positions; and (5) the parties were represented by counsel. The study database thus is limited to documented cases in which the parties conducted unsuccessful settlement negotiations and the parties' liability, if any, was ultimately decided by a judge, jury, or arbitrator.

The database excludes a few cases that otherwise might satisfy the five requirements above. Any trials concluded on technical or procedural grounds prior to an adjudication on the merits (for example, mistrials, directed verdicts, and defense verdicts based on motions for nonsuit, summary judgment, and judgment notwithstanding the verdict) were excluded. The outcome in those cases is a matter of law and frequently represents the losing attorney's error of law, as opposed to an attorney/client decision about mixed and disputed issues of both fact and law. Class actions also are excluded from the database since the relationship between attorneys and clients in those cases is too attenuated to assess attorney/client decision making. Cases in which typographical or reporting mistakes appeared on the face of the report or the parties' settlement positions were not adequately allocated among multiple parties were eliminated.

B. Variables Identified and Classified in Database

The variables in this study consist of three variables (AWARD, OFFER, and DEMAND) used to construct the dependent variable (DECISION ERROR) and 19 classes of independent variables (case types, two sets of party variables, 10 sets of attorney variables, damage claim, 998 offers of compromise, forum, alleged wrong, insurance coverage, and pretrial ADR procedures). Variable definitions and coding methods are described below.

1. Awards

The award in each case is the net financial award made by the judge, jury, or arbitrator. If an award to the plaintiff includes court costs and attorney fees in addition to the base award, the additional amounts were included. Gross awards were recalculated as necessary to adjust for comparative negligence allocations, "high-low" agreements, workers' compensation intervenor claims, and similar legally mandated adjustments. In cases where the defendant prevails (defense verdict), the award is classified as $0 unless fees or costs are awarded to the defendant. In those fee or cost award cases, the net result is recorded; for example, an award of $10,000 in attorney fees to a prevailing defendant is recorded as a –$10,000 result.

In this article, the term "net award" refers to any net award in favor of the plaintiff; the term "win rate" refers to the incidence of plaintiff net awards. The term "defense verdict" includes any award in favor of the defendant and against the plaintiff; a defense verdict does not imply or necessitate an ancillary award of costs, fees, or monetary sanctions to the defendant.

2. Settlement Demands and Offers

The study records the last settlement offer made before the jury renders a verdict, the judge issues a decision, or the arbitrator serves an award. Defendant offers are recorded as $0 when the *Verdict Search California* report states "none reported," "none," or "waiver of costs."

Cases in which a precise monetary amount could not be ascertained (e.g., "$100,000 offer with an indication of $125,000," "mid $800,000," or "$50,000 plus reasonable attorneys fees") were excluded from the study. If equitable relief was a component of the settlement negotiations ("$10,000 plus return of the car") or part of the award ("$15,000 to plaintiff and defendant to forthwith return the car"), the case also was excluded.[16]

---

[16]About 4,600 cases were reported in *Verdict Search California* during the 38-month study period. Twenty-nine percent of those cases were excluded because they reported pretrial settlements and thus did not proceed to an adjudicated outcome (coded as "mediated settlement" or "settlement" in the case data questionnaire), and 26 percent were excluded because the amount of settlement demands or offers was omitted or disputed, nonmonetary relief was sought, the parties were not represented by counsel, the trial was bifurcated and only the liability outcome was reported, or the case did not otherwise meet the selection criteria described in Section III.A and Section III.B.

Although the term "settlement offer" is used interchangeably to describe settlement proposals by both plaintiffs and defendants, this article usually employs the term "demand" to readily distinguish the plaintiff's offer ("demand") from the defendant's offer ("offer").

3. Case Type

Cases are classified by the type or nature of the legal claim asserted: contract, employment, fraud, intentional tort (nonfraud), medical malpractice, personal injury, premises liability, eminent domain,[17] product liability, negligence (nonpersonal injury), and other. These claims are tort, contract, and real property disputes; *Verdict Search California* does not report trials in other types of state court civil cases, for example, family law and probate matters.

Cross-complaints are treated as separate cases where the parties' settlement positions can be distinguished between the complaint and the cross-complaint. Where multiple plaintiffs or defendants have severable settlement positions or case outcomes, those cases also are coded as separate cases or excluded due to insufficient allocation information.

4. Parties

Both plaintiff and defendant parties are classified into nine categories: corporation, business (unincorporated business or possibly incorporated entity not specifically identified in the case facts as a corporation), insurer, male individual, female individual, female/male individuals, public entity, trust, or "other" party type.

5. Attorneys

Plaintiff and defendant attorneys are identified and coded by gender; firm size (whether among the 50 largest law firms in California as ranked by *The Daily Journal* in 2003 or 2004 or *California Lawyer* in 2005); years of experience after admission to the State Bar of California; academic rank of law school from which he or she graduated (whether a graduate of the nation's 20 best law schools as ranked by *U.S. News and World Report* in 2003, 2004, and

---

[17]The nominal positions of the parties in an eminent domain action (public entity as plaintiff and owner as defendant) are reversed in the data sets for consistency with their functional roles (owner seeks compensation from public entity) and eminent domain trial procedure (defendant owner assumes role of plaintiff in presenting its evidence first and commencing and concluding the argument). California Code of Civil Procedure § 1260.210(a).

2005); and diversity ranking of the law school from which he or she graduated (whether a graduate of the 20 law schools with the highest diversity index, as ranked by *U.S. News and World Report* in 2003, 2004, and 2005).[18]

The total number of attorneys included in the study database is 5,116, an estimated 17–21 percent of all California civil litigation attorneys.[19]

---

[18]California Top 50 Law Firms, Daily J. Extra, July 28, 2003, at 1–2; California Top 50 Law Firms, Daily J. Extra, July 26, 2004, at 14; Eric Cummins, The California 50, Cal. Law. (December 2005); Top 100 Law Schools, U.S. News & World Rep., retrieved Aug. 2, 2004, from ⟨http://www.usnews.com/usnews/edu/grad/rankings/law/brief/lawrank_brief.php⟩; Law School Diversity Index, U.S. News & World Rep., retrieved Aug. 2, 2004, from ⟨http://www.usnews.com/usnews/edu/grad/rankings/law/brief/lawdiv_brief.php⟩; Schools of Law, The Top 100 Schools and Law School Diversity, U.S. News and World Rep. 60–64 (2005). *Verdict Search California* reports only the name, firm, and location of the attorneys in each case. Data regarding other attorney characteristics, e.g., years of experience, law school, and law firm size, were obtained from membership records on the State Bar of California's public website, Martindale.com, the *Martindale-Hubbell Law Directory*, The Daily Journal's *California Directory of Attorneys*, and the websites of the subject law firms. In cases where more than two attorneys represent one party, only the first two listed attorneys are coded, except where multiple law firms represent a single party. In those multiple law firm conditions, the first attorney listed in the first two law firms is coded, to incorporate data from at least two different law firms representing that party. In public entity cases, however, the perfunctory listing of the county counsel in the first position is ignored and the next two listed attorneys from the county counsel's office are coded.

[19]Some attorneys appear in more than one case in the database, although this is an infrequent occurrence. Thus, the total number of individual attorneys is slightly less than 5,116. Although the State Bar of California does not maintain records regarding the precise number of civil litigation attorneys in California, 16 percent of the attorneys responding to its February 2006 survey identified civil litigation as their primary area or field of practice. Forty-five percent of the surveyed attorneys indicated a "secondary area of legal practice," and among that group 14 percent designated "civil litigation" as the secondary area. When asked what state bar section the members belonged to, only 7 percent of all surveyed members designated "litigation." Hertz Research, Final Report of Results, Member Services Survey, The State Bar of California—February 2006 17 (2006). Another source, Martindale-Hubbell, indicates that litigation attorneys comprise about 20 percent of all California attorneys, based on the total number of attorneys and litigation attorneys obtained from Martindale.com in June 2006 for the 20 largest cities in California. Attorneys in the Martindale-Hubbell directory can list more than one practice area. Hence, the Martindale-Hubbell data include attorneys who practice litigation exclusively and attorneys for whom litigation may be a secondary practice area. For the purposes of this study, acknowledging the limited data available and the possibility that attorneys for whom litigation is a peripheral practice area do not often try cases to verdict, the estimated percentage of California litigation attorneys is 16–20 percent of the total 154,073 active members as of June 15, 2006. Thus, the total estimated number of California litigation attorneys is 24,652–30,814. Since the total number of attorneys included in the study database is 5,116, the study attorneys represent an estimated 17–21 percent of California civil litigation attorneys.

6. Nature of Damages

In classifying damages, the study applies the nomenclature of cognitive psychology and behavioral economics theories, attempting to test the applicability of those theories to litigants' behavior. Damages, accordingly, are classified as either "current" damages (injuries, damages, and pain and suffering already incurred or sustained, variously described in other studies as out-of-pocket damages, expenditures, positive outlays, actual losses or expenses, and reimbursements) or "future" damages (comparatively remote claims for prospective loss not yet paid or incurred, such as projected medical expenses, future lost earnings, profits, anticipated pain and suffering, and royalties, variously referred to as "forgone gains," "failure to make gains," "negative losses," "expected economic gains," and "expectation interests").[20] In addition, punitive damages are classified separately where specifically sought.

7. Nature of Alleged Wrong

The study further classifies the underlying factual basis for the damage claim as an omission, commission, or both, again employing cognitive psychology and behavioral economics nomenclature to test "omission/commission bias," that is, the tendency to judge acts of commission as more blameworthy than acts of omission even when they cause identical economic harm. A collapsed lung allegedly caused by an assault, for instance, is coded as an act of commission, while the same injury, allegedly caused by an inattentive driver overlooking a stop sign, is classified as an act of omission. The classification is based on the plaintiff's allegations; an allegation of negligence alone is coded as an omission, while allegations of reckless, intentional, and malicious conduct, for example, are coded as commissions.

8. Forum

The type of adjudicator is coded as judge, arbitrator, or jury.[21]

---

[20]David Cohen & Jack L. Knetsch, Judicial Choice and Disparities Between Measures of Economic Value, in Choices, Values, and Frames, at 436–39 (Daniel Kahneman & Amos Tversky, eds., Press Syndicate of the University of Cambridge 2000).

[21]Gross and Syverud and Rachlinski limited their Verdict Search California data to jury verdicts. During the 10-year period after publication of their articles, the number of arbitration cases reported in Verdict Search California, as a percentage of all reported cases, has steadily

9. Section 998 Offers of Compromise

The study database records whether a party submitted a settlement demand or offer under California Code of Civil Procedure Section 998 (a "998 offer"). This statutory "offer of compromise" procedure, similar to Rule 68 of the Federal Rules of Civil Procedure, is intended to promote settlement by shifting certain costs onto a party who declines a 998 offer and fails to obtain a more favorable judgment at trial. The inclusion of this factor tests whether this cost-shifting sanction, as applied to these non-settling parties, promotes rational settlement positions or incites risk-taking negotiating behavior, as shown in Rachlinski's study of a "loser pays" litigation system and some behavioral economics studies of incentives and penalties.

10. Insurance

The existence of a reported insurer is coded in the database.[22]

11. Pretrial Dispute Resolution Procedures

The study database records whether a party reported participation in a pretrial alternative dispute resolution procedure, either nonbinding arbitration or mediation.[23]

---

increased, doubling between 1997 and 2006. Conversely, the percentage of reported jury verdicts decreased from 82 percent to 51 percent during that period, reflecting an increased reporting of arbitrations and settlements. In an email to a co-author dated May 31, 2007, the editor of Verdict Search California confirmed that the reporting and verification procedures for jury verdicts, bench decisions, and arbitration awards are identical.

[22]Attorneys may underreport insurance, as many Verdict Search California case reports omit the "Insurer(s)" section but indicate elsewhere that insurance existed. In the settlement demand part of the report, for instance, an attorney may report a "policy limits" demand but fail to report a carrier in the insurer section of the report. In cases where insurance is indicated but not explicitly reported in the insurer section, the existence of insurer was coded.

[23]Parties' participation in alternative dispute resolution procedures probably is underreported. Many case reports omit the "Arbitrator/Mediator" or "Neutral" section but indicate elsewhere that the parties participated in some form of ADR. The settlement demand part of the report, for instance, may state "$26,000 (Arbitration Award)" but omit the "Neutral" section. In cases where ADR participation is indicated but not expressly reported in the "Arbitrator/Mediator" or "Neutral" section, the case is coded for ADR participation.

C. Definition—Decision Error

Both Rachlinski and Gross and Syverud regard as error a party's failure to achieve a more favorable result at trial than could have been achieved by accepting the adverse party's demand or offer. Under this definition, a party errs when the award is the *same as or worse than* the demand or offer it declined. As Gross and Syverud state: "Any plaintiff who was offered as much as the verdict or more, and any defendant who could have settled for as much as the verdict or less, has lost."[24]

A "decision error," for purposes of this study, thus occurs when either a plaintiff or a defendant decides to reject an adversary's settlement offer, proceeds to trial, and finds that the result at trial is financially the same as or worse than the rejected settlement offer—the "oops" phenomenon. In absolute terms, the attorney and/or client made a decision error and the client sustained an unequivocal, quantifiable financial loss.[25] Decision error is strictly a mathematical calculation and does not signify or connote attorney negligence.

D. Methods

Having enumerated the variables that could affect decision making in settlement negotiations, we now identify the methodological approaches for understanding the most salient relationships in the *Verdict Search California* data. Decision error, our dependent variable, consists of three categories: plaintiff error, defendant error, and no error. Similarly, all our dependent variables are categorical; from the 19 classes of explanatory variables identified in the previous section (e.g., party or case type), we constructed 72 0/1 indicator variables (e.g., whether the plaintiff was a corporation or individual and whether the case type was a contract or medical malpractice dispute). We modeled the effect of these variables on decision error via multinomial logistic regression.

---

[24]Gross & Syverud (1996), supra, at 41–42.

[25]Parties, of course, may be motivated to litigate for reasons other than obtaining an optimal economic outcome. Gross and Syverud (1996), however, interviewed 735 attorneys in their data set and reported that "only three attorneys mentioned a desire for vindication as an explanation for why their case went to trial," and a "noneconomic motive" was highly infrequent." Supra, at 57.

As the number of explanatory variables is exceedingly large, we used a variety of techniques to determine which of the covariates were most pertinent for predicting decision error. For example, when we fit the model to the full set of covariates, a large number of the 146 coefficients[26] were not significant at any standard level. Deciding which of these variables to include in our model presented a challenge because, when conducting a large number of statistical tests, any standard level of statistical significance risks incorrectly rejecting several true null hypotheses of zero effect (i.e., the multiple comparisons problem). We attempted to obviate this problem in several separate (though related) ways. In general, our methods were both conservative and consistent in their results; thus, our goal—allowing the data to determine which covariates had the strongest statistical effect[27]—was well-served by them.

The first method we used to reduce our predictor set was to simply use the individual coefficient p values, with a Bonferroni adjustment for multiple comparisons. The Bonferroni threshold is quite high, requiring a variable in our data set to have a p value of 0.00034 to remain in the model. Not surprisingly, very few variables achieved this level of statistical significance (the indicator for medical malpractice cases, forum, and the two 998 offer of compromise variables).

Second, rather than looking at p values for individual coefficients, we looked at the p values generated by log-likelihood tests on our 19 variable classes (see Appendix), again taking multiple comparisons into account. When we did this, five variable groups remained: plaintiff attorney gender, case type, nature of damages, forum, and the two 998 offer of compromise variables.[28] Thus, this second method identified variables that were very similar to those identified by our first method.

Finally, we looked at the model chosen by the well-known Bayesian information criterion (BIC). This criterion is noted for finding parsimonious models that are consistent and practically efficient. Essentially, the BIC

---

[26](3 decision error types – 1 base type) * (72 variables + 1 intercept) = 146 coefficients.

[27]Had our goal been, for example, either prediction of decision error probability vector or the identification of all factors that influence decision error, we may have included more covariates. We commend these as fruitful areas for further research.

[28]We do not consider plaintiff attorney gender in the remainder of the article because in both the full model and the reduced model containing only these five variable groups, none of the individual plaintiff attorney gender coefficients was statistically significant.

assigns a score to a model based on the quality of the fit along with a penalty for the number of variables used. Due to this penalty factor, the BIC can be robust to overfitting and avoid selection of spurious variables (as would be done if one ran the full model and took all variables with p values less than 0.05). Because there were 2^{73} (approximately 10^{22}) different possible models, we could not evaluate them all and choose the one with the best BIC. Instead, we used a procedure that evaluated models one by one until the BIC stopped improving; since roughly the same variables were selected when we provided the procedure with different starting points, we were satisfied that the key predictor variables were identified. We present one such model in Table 4 and note that it largely agrees with the results of the two other models mentioned above.

Because multinomial logistic regression coefficients can be difficult to interpret,[29] we use univariate and bivariate tables (in addition to the regression output table) to summarize the effects of indicator variables identified by the multivariate analysis as most significant. The advantage of this approach, beyond simplifying the explanation of the relationships, is that it also permits a presentation of the *cost* of error, not just the *kind* of error, precisely as described by Rachlinksi in his work on this subject.

IV. Study Results

The study results are summarized in this order: Section IV.A presents the aggregate study results, compares those results with prior studies, and

---

[29]The multinomial logit model assumes that the conditional probability of a given class is of the form:

$$P(Y = j|X) = \frac{\exp(X\beta_j)}{\sum_{i=1}^{J} \exp(X\beta_i)},$$

where $j = 1, \ldots, J$ where the vector b_1 is assumed to be zero without loss of generality in order to identify the model. The numbering of the categories is arbitrary and in our case we take "no error" to be Category 1, "plaintiff error" to be Category 2, and "defendant error" to be Category 3. This model specification implies that the log odds of plaintiff error (or defendant error) relative to the base category (no error) follows a linear function. That is, the regression coefficients can be interpreted in the ordinary way when applied to the log odds. Since all our covariates are categorical variables, the estimated coefficients show the change in the log odds on a case for which this variable is true compared to one for which it is false.

provides a historical context for those results; Section IV.B explains the multivariate analysis and discusses the effects of four key variables (offers to compromise, case type, forum, and nature of damages); and Section IV.C summarizes and compares the results from the attorney/mediator sample.

A. Decision Error and its Costs—General Overview

To facilitate comparisons with earlier works and to highlight the robustness of results across alternative formulations and samples, we have chosen to summarize our findings using the tabular framework adopted by Rachlinski (1996). It succinctly captures both the prevalence of decision error by plaintiffs and defendants and the magnitude of those errors. Multiplying those two aggregate measures—decision error (in percent) and mean cost of error—yields an estimate of the expected cost of each party's error.

1. Aggregate Results

As indicated in Table 1, the incidence of decision error for plaintiffs is higher than for defendants, but the cost of decision error is higher for defendants than for plaintiffs. In this sample of adjudicated cases, plaintiffs committed decision error, receiving an award less than or equal to the last offer made by the defendant, in 61.2 percent of the cases. By contrast, defendants committed decision error in 24.3 percent of the cases.[30] Nonetheless, there is a substantial difference in mean cost of error between plaintiffs and defendants ($43,100 and $1,140,000, respectively[31]). Given the relatively large discrepancy between the parties' mean cost of error, it is not surprising that the expected cost of error is greater for defendants by a factor of 10.

The findings from our sample are qualitatively similar to those of Rachlinski (1996). Some quantitative differences, however, are noteworthy. Though defendants' decision error did not change substantially (24.3 percent in our sample compared with 23.0 percent in Rachlinski's sample), plaintiffs' decision error rose from 56.1 percent to 61.2 percent, with a

---

[30]Decision error rates are significantly different at the 0.01 level.

[31]Significantly different at the 0.01 level.

Table 1: Decision Error and Cost of Error—All Cases

	Decision Error					*Cost of Error*	
Error Type	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
No error	296	14.5%	467.8	918.6	191.3	NA	NA
Plaintiff error	1250	61.2%	5.7	565.8	48.7	43.1	26.4
Defendant error	497	24.3%	1,910.9	770.9	222.4	1,140.0	277.3

corresponding decline in "no error" cases from 20.9 percent to 14.5 percent. The largest change was in defendants' mean cost of error, with mean cost of error rising from $354,900 to $1,140,000 and expected cost of error rising from $81,600 to $277,300. Even after adjusting for inflation, there was a 78 percent rise in defendants' mean cost of error and an 89 percent increase in defendants' expected cost of error. Notwithstanding the increase in plaintiffs' decision error, their mean cost of error after adjusting for inflation was lower in the 2003–2005 period relative to Rachlinski's results in the 1981–1988 period. The declines in plaintiffs' real mean cost of error and real expected cost of error were 14 percent and 5 percent, respectively.

Our sample findings also parallel the decision error rates compiled by Gross and Syverud (1996). The plaintiffs' decision error rate of 61.2 percent in our study nearly replicates Gross and Syverud's conclusion that "plaintiffs were clear losers in most of these trials, at least in economic terms—61% overall in 1985–86, 65% in 1990–91."[32] The defendants' decision error rate of 24.3 percent in our study closely reflects the 25 percent and 26 percent defense error rates in Gross and Syverud's 1985–1986 and 1990–1991 samples, respectively.

Defendants' relatively high mean cost of error in our study ($1,140,000 for defendants vs. $43,100 for plaintiffs) is consistent with the "framing" effects discerned by both Gross and Syverud and Rachlinski. Gross and Syverud found that plaintiffs usually are more risk averse than defendants, and Rachlinski concluded that "plaintiffs behavior was, on balance, risk-averse," while defendants' behavior "can only be described as risk-seeking."[33]

---

[32]Gross and Syverud (1996), supra, at 42.

[33]Gross and Syverud (1991), supra, at 381; Rachlinski (1996), supra, at 159.

2. Historical Context

To provide a historical context for the overall findings, we abstracted from *Jury Verdicts Weekly* plaintiff demands, defendant offers, and awards for a 40-year period, at five-year intervals, from 1964 through 2004. All cases reported in the first quarter of each pertinent year were included if they met the selection criteria employed for cases in the primary study group. Though the samples are smaller—ranging from 159 cases to 366 cases per quarter—they provide insight into some trends over that 40-year period. The results are displayed in Table 2.

Despite some volatility over time, the incidence of decision error is greater at the end of the period than at the beginning. That is, the amount of "no error" drops from 27.2 percent and 25.2 percent in 1964 and 1969, respectively, to 17.5 percent and 14.0 percent for the years 1999 and 2004, respectively.

The cost of decision error is substantially greater at the end of the period.[34] Converting the nominal values in Table 2 to real values (in 1964 dollars) demonstrates the dramatic rise in the magnitude of the parties' errors over time.

Table 3 provides a summary in which the values are clustered into groups of three years, reflecting the subperiods 1964–1974, 1979–1989, and 1994–2004. From the earliest period to the latest period, plaintiffs experienced nearly a three-fold real (i.e., inflation-adjusted) increase in cost of error (both mean cost and expected cost of error), whereas defendants experienced in excess of a 14-fold real increase in mean cost of error.[35]

---

[34]Civil discovery in California changed significantly during this period due to liberal interpretations of the Civil Discovery Act of 1957 and the enactment of the Civil Discovery Act of 1986. These changes were intended to encourage settlements, reveal the strengths and weaknesses of an adversary's case, eliminate surprise, and generally end the "trial by ambush" era. See Fairmont Ins. Co. v. Superior Court, 22 Cal. 4th 253 n.2 (2000); Greyhound Corp. v. Superior Court, 56 Cal. 2d 355 (1961). Although those objectives may well have been achieved in the California cases that settle, the historical sample and the primary data set indicate that for nonsettling parties, the surprises are neither less frequent nor less costly.

[35]From the earliest period, 1964–1974, to the latest period, 1994–2004, the real cost of error and real expected cost of error for both plaintiffs and defendants are significantly different at the 0.01 level. The p values for these tests and all others involving covariates were calculated using permutation tests. We preferred permutation tests due to the paucity of assumptions required to use them (e.g., no normality assumptions are required). Since many of our variables are highly skewed, such assumptions would likely be inappropriate.

Table 2: Decision Error and Cost of Error—Historical Samples

		Decision Error					Cost of Error	
Year	*Error Type*	*# of Cases*	*% of Cases*	*Mean Award ($1,000's)*	*Mean Demand ($1,000's)*	*Mean Offer ($1,000's)*	*Mean Cost of Error ($1,000's)*	*Expected Cost of Error ($1,000's)*
1964	No error	50	27.2%	11.5	22.1	4.0	NA	NA
1964	Plaintiff error	99	53.8%	2.0	11.5	3.1	1.2	0.6
1964	Defendant error	35	19.0%	19.4	13.5	5.7	5.9	1.1
1969	No error	40	25.2%	26.2	35.4	15.6	NA	NA
1969	Plaintiff error	79	49.7%	3.0	21.6	4.8	1.8	0.9
1969	Defendant error	40	25.2%	62.2	34.9	9.9	27.3	6.9
1974	No error	48	14.7%	32.4	52.1	12.9	NA	NA
1974	Plaintiff error	214	65.4%	1.7	27.8	7.4	5.7	3.7
1974	Defendant error	65	19.9%	132.4	89.8	16.3	42.6	8.5
1979	No error	39	19.3%	20.5	51.8	9.8	NA	NA
1979	Plaintiff error	117	57.9%	1.8	79.2	8.4	6.6	3.8
1979	Defendant error	46	22.8%	132.7	65.0	23.0	67.7	15.4
1984	No error	25	11.3%	75.1	142.6	18.4	NA	NA
1984	Plaintiff error	138	62.4%	2.7	199.5	21.0	18.4	11.5
1984	Defendant error	58	26.2%	851.2	222.7	30.8	628.4	164.9
1989	No error	26	15.0%	878.7	1,552.8	165.8	NA	NA
1989	Plaintiff error	109	63.0%	4.6	296.0	43.0	38.4	24.2
1989	Defendant error	38	22.0%	1,006.7	460.2	79.3	546.5	120.0
1994	No error	20	10.2%	314.4	493.8	123.9	NA	NA
1994	Plaintiff error	133	67.9%	4.0	366.2	26.4	22.4	15.2
1994	Defendant error	43	21.9%	1,550.6	430.0	95.3	1,120.6	245.8
1999	No error	64	17.5%	219.0	454.6	43.1	NA	NA
1999	Plaintiff error	220	60.1%	34.2	668.3	79.9	45.7	27.4
1999	Defendant error	82	22.4%	2,798.7	539.0	146.6	2,259.8	506.3
2004	No error	25	14.0%	221.1	502.3	79.5	NA	NA
2004	Plaintiff error	117	65.7%	12.9	601.1	53.7	40.8	26.8
2004	Defendant error	36	20.2%	1,519.4	870.3	651.0	649.1	131.3

Table 3: Cost of Error in Constant 1964 Dollars

Period Type of Error	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
1964, 1969, 1974		
Plaintiff error	2.6	1.5
Defendant error	20.5	4.3
1979, 1984, 1989		
Plaintiff error	5.9	3.6
Defendant error	122.5	29.2
1994, 1999, 2004		
Plaintiff error	7.0	4.4
Defendant error	300.6	65.4

B. Decision Error and its Costs—Results from the Multivariate Analysis

Table 4[36] gives the estimated effect of a given variable on the log odds of plaintiff decision error (defendant decision error) relative to no decision error. Though we will not focus on it at length, there are a few points worth noting. Examination of individual p values is not appropriate since the model presented here was selected by searching over the model space; that said, the coefficients appear to be statistically significant. In addition, we note that the coefficients imply changes in the predicted probability of an outcome (i.e., plaintiff decision error, defendant decision error, or no error) that comport well with legal intuition. This can be seen by completing some simple numerical calculations to back out the implied probabilities from the log odds.

Before proceeding with the more illuminating univariate and bivariate tables, it is worthwhile to discuss the variables briefly. The predictor variables tend to fall into two types of categories that can be thought of as "actor" and "context" related. Actor variables describe the type of plaintiff or defendant (e.g., corporation, individual, unincorporated business entity) and the attorneys (e.g., gender, law firm size, law school ranking, experience). Context variables, on the other hand, are the conditions under which the actors—attorneys and parties—make settlement decisions, for example, whether 998 offers were served, the forum in which a case is being tried, the type of case,

[36]This table is for the model selected by BIC. As mentioned in the text, the models selected by significance tests were largely similar so it would be redundant to present them all.

Table 4: Decision Error Multinomial Logistic Regression Results

Variable: Effect on Party's DE	*Value*	*s.e.*	t *Value*
Intercept: P	–0.538	0.341	–1.578
Intercept: D	–0.067	0.310	–0.215
P 998 offer: P	–0.503	0.175	–2.870
P 998 offer: D	1.091	0.183	5.956
D 998 offer: P	0.930	0.175	5.303
D 998 offer: D	–0.374	0.201	–1.856
Forum—bench: P	1.528	0.445	3.436
Forum—bench: D	0.574	0.417	1.376
Forum—jury: P	2.123	0.328	6.474
Forum—jury: D	0.276	0.292	0.945
Case type—med mal: P	1.932	0.323	5.974
Case type—med mal: D	0.733	0.351	2.088
Case Type—contract: P	–0.030	0.286	–0.105
Case Type—contract: D	0.922	0.293	3.151
Case type—personal injury: P	–0.752	0.157	–4.794
Case type—personal injury: D	–0.272	0.179	–1.522
Damages—punitive: P	–0.437	0.293	–1.494
Damages—punitive: D	0.458	0.304	1.503
Residual deviance: 3319.733 on 4,016 degrees of freedom			
Log-likelihood: –1659.867 on 4,016 degrees of freedom			

or the nature of alleged damages. Our final models selected only context variables, no actor variables having been selected by the statistical procedures previously described.

By far the most important variables were those indicating whether the plaintiff or the defendant had served 998 offers. All the variable selection methodologies identified these variables as very strong predictors. In addition, some of the case type variables were identified as being important. Particularly, medical malpractice cases, contract cases, and personal injury cases were important factors for predicting whether one of the parties made a decision error. Other variables that were useful for predicting the incidence of decision error were the types of damages alleged as well as the forum in which the case was resolved.

The results shown below in the tabular format are qualitatively quite similar to the regression results. We will focus on 998 offers and case type since they are the most interesting and dramatic, though we will also discuss the forum and nature of damages variables. In particular, the results on 998 offers will be compared to Rachlinski's results for "loser pays" legislation. Though loser pay schemes and 998 offers differ in structure, they are conceptually similar in imposing financial penalties dependent on the case

outcome. In addition, the results on type of case will be compared to the case type analysis performed by Gross and Syverud. However, as we will indicate, one must be careful comparing the results by case type because case coding methods are not identical and this study includes bench trials and arbitration awards, while prior studies were limited to jury trials.

1. Effects of 998 Offers

California Code of Civil Procedure Section 998 is a statutory cost-shifting mechanism designed to encourage settlement and penalize unreasonable settlement positions. Any party can serve a written "998 offer" on the other party while a case is pending, up to 10 days before trial commences.[37] A party who does not accept an adverse party's 998 offer and obtains a worse result at trial may be liable for the adverse party's court costs, expert witness fees, and, in personal injury cases, interest from the date of the offer. "The purpose of section 998," the court held in *Taing v. Johnson Scaffolding Co.*,[38] "is to encourage the settlement of lawsuits before trial by penalizing a party who fails to accept a reasonable offer from the other party."[39]

The multivariate analysis indicated the importance of 998 offers in explaining decision error for both parties. The results of the four possible 998 conditions (no 998 offer, plaintiff only 998 offer, defendant only 998 offer, and dual plaintiff/defendant 998 offers) are shown in the following four related tables. Table 5, Panel 5a summarizes the results for those cases in which no 998 offers were served. Representing 1,196 cases, or 59 percent of the entire sample, this panel indicates that the incidence of decision error by both plaintiffs and defendants in the "no 998 offer" condition is not substantially different from the overall study results presented in Table 1.

We compare the results for those cases in which one or both parties submitted a 998 offer with the "no 998 offers" in Table 5, Panel 5a. There were 847 cases (41 percent of the sample) in which one or both parties

---

[37]The "offer of compromise" under Section 998 must expressly refer to the statute or otherwise notify the offeree that costs otherwise allowed to a prevailing party may be reduced or augmented if the offer is not accepted. See Stell v. Jay Hales Dev. Co., 11 Cal. App. 4th 1214, 1231, 1232 (1992). An oral offer purportedly made under Section 998, even if placed on the record during a deposition, does not satisfy the statutory requirements. Saba v. Crater, 62 Cal. App. 4th 150, 153 (1998).

[38]9 Cal. App. 4th 579, 583 (1992).

[39]*Taing* was distinguished in Bihun v. AT&T Info. Sys., 13 Cal. App. 4th 976 (1993).

Table 5: Decision Error and Cost of Error—The Effects of 998 Offers

	Decision Error					*Cost of Error*	
Error Type	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
Panel 5a: No 998 Offers							
No error	195	16.3%	573.8	1,173.8	249.4	NA	NA
Plaintiff error	733	61.3%	8.6	647.2	53.3	44.7	27.4
Defendant error	268	22.4%	2,115.1	815.7	174.5	1,299.4	291.2
Panel 5b: 998 Offers by Plaintiffs Only							
No error	34	12.5%	246.2	457.5	67.7	NA	NA
Plaintiff error	112	41.2%	15.9	450.7	35.1	19.2	7.9
Defendant error	126	46.3%	2,358.1	988.0	400.3	1,370.1	634.7
Panel 5c: 998 Offers by Defendants Only							
No error	29	10.2%	265.5	407.4	108.6	NA	NA
Plaintiff error	236	83.1%	(0.3)	562.2	39.2	39.5	32.8
Defendant error	19	6.7%	2,192.5	1,088.7	437.3	1,103.9	73.9
Panel 5d: 998 Offers by Both Plaintiffs and Defendants							
No error	38	13.1%	276.2	411.5	66.8	NA	NA
Plaintiff error	169	58.1%	(5.5)	294.4	51.4	57.0	33.1
Defendant error	84	28.9%	525.1	230.6	59.5	294.5	85.0

served 998 offers: 272 by plaintiffs only, 284 by defendants only, and 291 by both parties. The results for those subsamples are contained in Panels 5b, 5c, and 5d, respectively. Jointly, the table supports the notion that, other things being equal (or at the margin), serving a 998 offer reduces both decision error and mean cost of error for the serving party, though it increases decision errors and expected cost of error for the recipient party. Interestingly, total decision error always increases in the presence of a 998 offer (i.e., "no error" is always a lower percent when 998 offers are served). This is due to the fact that the reduction in the serving party's decision error is more than offset by the rise in the recipient party's decision error. The effect on overall cost of error depends on who is serving and receiving the 998 offer—this owing to the fact that the magnitudes of change in cost of error for defendants are substantial both when making and receiving 998 offers, and relatively more so when receiving a 998 offer.

As is evident from Table 5, Panel 5b, a plaintiff 998 offer reduces both decision error and cost of error for plaintiffs, but raises both types of errors for defendants (i.e., more risk-taking behavior by defendants).[40] Similarly, Panel 5c demonstrates that a defendant 998 offer reduces both decision error and cost of error for the defendant. The presence of a defendant 998 offer, however, sharply increases plaintiffs' decision error rates. Although there is a slight reduction in plaintiffs' mean cost of error when defendants serve a 998 offer, the expected cost of error rises because of the much higher degree of plaintiff decision error (i.e., a somewhat lower mean multiplied by a much higher decision error percentage).[41]

When both parties serve 998 offers, theory cannot predict the final result; the result is an empirical issue. Table 5, Panel 5d provides the results for the dual 998 offer condition. For plaintiffs in the dual 998 offer condi-

---

[40]Except for defendant mean cost of error ($1,299,400 vs. $1,370,100), all differences are statistically significant. That is, the reduction in decision error in cases where the plaintiffs made 998 offers relative to those cases in which no 998 offers were made (41.2 percent vs. 61.3 percent), and the rise in decision error among defendants in those same cases (46.3 percent vs. 22.4 percent) are both significant at the 0.01 level. The reductions in plaintiffs' mean cost of error and expected mean cost of error ($44,700 vs. $19,200 and $27,400 v. $7.900) as well as the rise in defendants' expected cost of error ($291,200 vs. $634,700) are all significant at the 0.02 level or lower.

[41]The reduction in defendants' decision error (6.7 percent vs. 22.4 percent) as well as the rise in plaintiffs' decision error (83.1 percent vs. 61.3 percent) are significant at the 0.01 level. However, other than the value of defendants' expected cost of error, the differences in other values of mean cost and expected mean cost are not significant at the 0.05 level.

tion, there is a slight reduction in decision error compared with the "no 998 offer" condition (58.1 percent vs. 61.3 percent) and a slight increase in the mean cost of error ($57,000 vs. $44,700) and expected cost of error ($33,100 vs. $27,400). For defendants in the dual 998 offer condition, there is an increase in the defendants' decision error compared with the "no 998 offer" condition (28.9 percent vs. 22.4 percent) and a more substantial decrease in the mean cost of error ($294,500 vs. $1,299,400) and expected cost of error ($85,000 vs. $291,200).[42]

The purpose of 998 offers is to encourage settlements by imposing financial penalties on parties who take unreasonable settlement positions. Cost-shifting statutory schemes like the 998 offer to compromise and its federal counterpart, Rule 68, however, may actually induce risk taking by the parties and may provoke the gambling mentality they are intended to curb. Rachlinski's study of "loser pays" systems, enacted to deter meritless lawsuits and increase settlements, found that "by raising the stakes at trial, the loser-pays system makes litigation itself more valuable and can discourage settlement."[43] In this study, the 998 offer procedure may produce that unintended consequence as well. (This observation, of course, is limited to this study of adjudicated cases; 998 offers may be effective in inducing reasonable conduct in settled cases.) Higher decision error rates in this study were correlated with the receipt of a 998 offer; this raises the question of whether the 998 statutory scheme actually heightens risk-seeking behavior by the recipient party, contrary to the legislative intent.[44]

---

[42]None of the differences for plaintiffs (decision error, mean cost of error, or expected mean cost of error) is significant at the 0.05 level, though all the differences for defendants are significant at the 0.05 level.

[43]Rachlinski, supra, at 161.

[44]The reduction in the "no decision error" rate (i.e., the increase in overall decision error) in the presence of defendant offers relative to no 998 offers (10.2 percent vs. 16.3 percent) is significant at the 0.01 level. Though the changes in "no decision error" rates under plaintiff 998 offers (12.5 percent vs. 16.3 percent) and joint 998 offers (13.1 percent vs. 16.3 percent) are not statistically significant at the 0.05 level (with a two-sided test), they are lower rather than higher, meaning that the point estimates indicate greater decision error rather than reduced decision error as intended by the legislature (a one-sided test would imply a p value of zero for all three comparisons).

One may argue that a 998 offer does not cause the risk-taking behavior but, rather, is propounded to curb or penalize extreme settlement positions after an adverse party has manifested unreasonable settlement behavior. Under this argument, a 998 offer may be a reaction to, not a cause of, an adverse party's risk-taking behavior. The weakness in this argument is that it overlooks the underlying intent of the 998 statutory procedure: to promote reasonable settlement behavior by imposing a financial penalty on unreasonable settlement positions, whether the recipient party is a reckless or a rational decision maker. Although 998 offers may have a salutary effect on those cases that settle, in this sample of adjudicated cases the service of a 998 offer was correlated with significantly higher decision error by the recipient party.

2. Effects of Case Type

Under the Priest and Klein "fifty percent implication," one expects win rates and decision error rates to be balanced between the parties and unaffected by the case type. Plaintiffs would win 50 percent of their cases, regardless of case types and, with respect to decision error, plaintiffs and defendants would be "equally successful at predicting the outcomes of the cases."[45] Priest and Klein note that "the most important assumption of the model is that potential litigants form rational estimates of the likely decision, whether it is based on applicable legal precedent or judicial or jury bias."[46] Their 50 percent implication further assumes that litigation costs are relatively high compared to settlement costs, the application of legal standards is predictable, both parties can predict outcomes with "equal precision," and the stakes are "symmetrical" to the parties, that is, gains and losses from litigation "are equal to both parties."[47] The assumptions and predictive capacity of the Priest and Klein model, however, are challenged by the study data showing that both win rates and error rates vary widely with different types of cases, as shown in Tables 6 and 7.

---

[45]Gross and Syverud, supra, at 325.

[46]Priest & Klein (1984), supra, at 4.

[47]Priest & Klein (1984), supra, at 5, 12, 14, 19, 20, 24.

Table 6: Win Rates, Mean Awards, and Mean Offers by Type of Case

Case Type	*Win Rate*	*# of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*
Eminent domain	100.0%	12	5,231.35	5,249.75	3,588.78
Contract	62.6%	174	1,356.15	1,323.05	98.41
Fraud	61.4%	57	2,731.81	1,473.90	132.04
Personal injury	60.9%	834	345.60	368.45	101.64
Employment	51.1%	139	703.74	900.48	86.88
Other	42.9%	28	275.86	807.57	65.64
Negligence (non-PI)	42.6%	94	823.84	1,072.11	93.23
Premises liability	36.9%	268	627.77	742.83	134.06
Intentional tort	35.2%	179	315.35	737.16	50.65
Products liability	30.2%	53	494.69	1,174.06	131.90
Medical malpractice	19.5%	364	234.80	505.68	31.28

In general, high plaintiff error rates are associated with cases in which contingency fee arrangements are common, for example, personal injury (53 percent error rate) and medical malpractice (81 percent error rate), while low error rates are associated with cases in which contingency fee arrangements are uncommon, for example, contracts (44 percent error rate) and eminent domain (42 percent error rate).[48] On the defense side, high error rates are noted in cases where insurance coverage is generally unavailable, for example, contracts (44 percent) and fraud (40 percent), while low error rates are associated with cases in which insurers are more likely to represent defendants, for example, premises liability (17.5 percent error rate) and personal injury (26.3 percent error rate).

---

[48]The higher error rates attendant to plaintiff contingency fee cases may reflect optimistic overconfidence. In one study, lawyers retained on a contingency basis showed the same level of confidence about case outcomes as other lawyers, although the contingency basis attorneys won only 42 percent of their cases compared with an overall 56 percent win rate. In general, that study found that lawyers' predictions regarding whether they would win their case "showed no predictive validity" and were "hardly above chance." They exhibited a marked "overextremity bias (underprediction of success for low probabilities and overprediction of success for high probabilities)." J. Goodman-Delahunty, P.A. Granhag & E.F. Loftus, How Well Can Lawyers Predict Their Chances of Success? Unpublished manuscript (University of Washington 1998), cited in Derek J. Koehler, Lyle Brenner & Dale Griffin, The Calibration of Expert Judgment: Heuristics and Biases Beyond the Laboratory, in Heuristics and Biases: The Psychology of Intuitive Judgment 705, 706 (Thomas Gilovich, Dale Griffin & Daniel Kahneman, eds., Press Syndicate of the University of Cambridge 2002). For other results regarding attorneys' predictive capabilities, see Elizabeth F. Loftus & Willem A. Wagenaar, Lawyers' Predictions of Success, 28 Jurimetrics 437 (1988).

Table 7: Decision Error and Cost of Error—By Case Type

		Decision Error					Cost of Error	
Case Type	*Error Type*	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
Eminent domain	No error	3	25.0%	14,946.7	15,087.3	9,806.0	NA	NA
	Plaintiff error	5	41.7%	1,138.4	1,517.0	1,210.5	72.1	30.0
	Defendant error	4	33.3%	3,061.1	2,537.5	1,898.8	523.6	174.5
Contract	No error	20	11.5%	1,022.1	2,138.9	60.1	NA	NA
	Plaintiff error	77	44.3%	(58.3)	1,105.5	86.6	144.9	64.1
	Defendant error	77	44.3%	2,857.3	1,328.6	120.1	1,528.7	676.5
Fraud	No error	7	12.3%	329.9	501.4	68.1	NA	NA
	Plaintiff error	27	47.4%	(14.5)	766.3	119.9	134.4	63.7
	Defendant error	23	40.4%	6,686.8	2,600.6	165.8	4,086.2	1,648.8
Personal injury	No error	171	20.5%	167.6	326.3	67.7	NA	NA
	Plaintiff error	444	53.2%	13.8	302.3	46.0	32.2	17.2
	Defendant error	219	26.3%	1,157.4	535.4	240.9	622.0	163.3
Employment	No error	23	16.5%	499.3	1,744.9	207.0	NA	NA
	Plaintiff error	71	51.1%	(1.3)	878.9	63.4	64.8	33.1
	Defendant error	45	32.4%	1,920.7	503.0	62.5	1,417.7	459.0
Other	No error	2	7.1%	91.0	137.5	17.4	NA	NA
	Plaintiff error	18	64.3%	1.9	978.4	31.6	29.6	19.0
	Defendant error	8	28.6%	938.4	590.7	154.4	347.7	99.3
Negligence (non-PI)	No error	14	14.9%	1,537.8	2,184.6	114.2	NA	NA
	Plaintiff error	62	66.0%	(7.2)	686.8	74.9	82.1	54.2
	Defendant error	18	19.1%	3,131.1	1,534.1	140.1	1,597.0	305.8
Premises liability	No error	37	13.8%	333.9	1,202.1	175.3	NA	NA
	Plaintiff error	184	68.7%	3.0	603.4	49.1	46.1	31.7
	Defendant error	47	17.5%	3,305.0	927.0	434.0	2,378.0	417.0
Intentional tort	No error	17	9.5%	274.7	1,375.9	28.6	NA	NA
	Plaintiff error	124	69.3%	(6.1)	715.2	37.4	43.4	30.1
	Defendant error	38	21.2%	1,382.4	522.9	103.9	859.4	182.4
Products liability	No error	6	11.3%	959.8	1,158.3	51.0	NA	NA
	Plaintiff error	38	71.7%	(8.1)	1,222.4	64.5	72.6	52.0
	Defendant error	9	17.0%	2,307.7	980.3	470.6	1,327.3	225.4
Medical malpractice	No error	15	4.1%	329.5	448.9	88.0	NA	NA
	Plaintiff error	294	80.8%	(0.6)	513.1	14.6	15.2	12.3
	Defendant error	55	15.1%	1,467.6	481.4	105.2	986.2	149.0

In general, an inverse relationship exists between plaintiff decision error rates and win rates. Plaintiff decision error is lowest in cases with high win rates and highest in cases with low win rates. Contract cases, for instance, have a 44.3 percent decision error rate and a 62.6 percent win rate, while medical malpractice cases have an 80.8 percent plaintiff decision error rate and a 19.5 percent win rate. For defendants, the pattern generally is reversed; high decision error rates are evident in high win rate cases.

The decision error rates, when classified by identical case types, appear to be roughly consistent with Gross and Syverud's data for 1985–1986 and 1990–1991 cases. In Gross and Syverud's study, for instance, plaintiffs in medical malpractice cases were "clear losers" in 71 percent and 78 percent, respectively, of the cases, compared with a 80.8 percent decision error rate in our study. Defendants' decision error rate in Gross and Syverud's study was 17 percent and 16 percent, respectively, compared with 15.1 percent in our study. The results in products liability cases are more disparate, but reflect similar qualitative differences between plaintiff and defendant decision error. Gross and Syverud's data show plaintiffs in products liability cases either recovered nothing or less than the defendants' offer in 64 percent and 61 percent of the cases, compared to plaintiffs' decision error rate of 68.7 percent in our study. Defendants, on the other hand, committed decision error in 25 percent and 32 percent of the Gross and Syverud cases, contrasted with 17 percent in our study.

3. Effects of Forum

The forum variables are jury trials, bench trials, and arbitration. Under the Priest and Klein model, one would expect decision error rates to be balanced between the parties regardless of the forum; the forum itself would not appear to affect the hypothesis or its premises. The multivariate analysis, however, indicates that forum affects decision error rates. The effect of forum on decision error rates and cost of error is presented in Table 8.

Most cases (90 percent) were tried to juries, while the remaining cases were divided about evenly between bench trials and arbitrations. Due to the prevalence of jury trials, the outcomes for jury trials are similar to the overall results presented in Table 1.

Both plaintiffs and defendants displayed remarkably different decision error rates in different forums. Defendants committed substantially less decision error in jury trials relative to bench trials (22.1 percent vs. 42.6

Table 8: Decision Error and Cost of Error—By Forum

	Decision Error					*Cost of Error*	
Error Type	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
Panel 8a: Arbitration							
No error	25	25.8%	249.4	424.0	66.3	NA	NA
Plaintiff error	28	28.9%	(1.1)	1,099.5	5.6	6.7	1.9
Defendant error	44	45.4%	748.8	359.8	71.1	389.0	176.4
Panel 8b: Bench Trials							
No error	16	14.8%	199.2	513.4	30.3	NA	NA
Plaintiff error	46	42.6%	(7.4)	287.8	16.2	23.6	10.1
Defendant error	46	42.6%	2,427.9	1,302.5	519.0	1,125.3	479.3
Panel 8c: Jury Trials							
No error	255	13.9%	506.0	992.5	213.7	NA	NA
Plaintiff error	1176	64.0%	6.3	564.0	51.0	44.7	28.6
Defendant error	407	22.1%	1,978.1	755.3	205.2	1,222.8	270.8

percent). By contrast, plaintiff decision error was considerably higher in jury trials relative to bench trials (64.0 percent vs. 42.6 percent).[49]

In arbitration cases, decision error rates for both plaintiffs and defendants differed substantially from their rates in jury cases. Defendants' decision error rate (45.4 percent) was similar to their error rate in bench trials (42.6 percent) but considerably more than in jury trials (22.1 percent).[50] Plaintiffs' decision error in arbitration cases (28.9 percent) was notably lower than in either bench trials (42.6 percent) or jury trials (64.0 percent).[51] The total amount of decision error, moreover, is much lower in arbitration than in either bench or jury trials, with "no error" being 25.8 percent in arbitration relative to 14.8 percent in bench trials and 13.9 percent in jury trials.[52]

4. Effects of Damages Claim

Damages are characterized in the database as (1) "current" damages, representing injuries and damages already sustained, (2) "future" damages, representing prospective losses not yet paid or sustained, and (3) punitive or exemplary damages. A plaintiff in a personal injury suit against an intoxi-

---

[49]Both differences in decision error rates are significant at the 0.01 level. Defendants' mean cost of error was roughly the same in jury and bench trials, and while the expected cost of error was estimated to be much lower in jury trials than bench trials (due to the drop in decision error for jury trials), the difference is not significant at the 0.05 level. Though the difference in plaintiffs' mean cost of error between jury and bench trials ($44,700 vs. $23,600) is not significant at the 0.05 level, the difference in the expected cost of error between them is significant at the 0.01 level ($28,600 in jury trials vs. $10,100 in bench trials).

[50]Defendants' decision error rate of 45.4 percent in arbitration cases was significantly different from their 22.1 percent decision error rate in jury trials (at the 0.01 level), while not being significantly different from the decision error rate of 42.6 percent in bench trials (even at the 0.05 level). Though defendants' estimated mean cost of error ($389,000) in arbitration cases was substantially less than in either bench trials ($1,125,300) or jury trials ($1,222,800), neither difference is significant at the 0.05 level. Defendants' expected cost of error was also smallest in cases decided by arbitrators.

[51]Plaintiffs' decision error rate of 28.9 percent in arbitration cases was significantly different from their 42.6 percent decision error rate in jury trials (at the 0.05 level) and from their decision error rate of 64.0 percent in bench trials (at the 0.01 level). Though neither the difference between plaintiffs' mean cost of error in arbitration versus bench trials ($6,700 vs. $23,600) nor their expected cost of error in those forums ($1,900 vs. $10,100) was significant at the 0.05 level, the differences between arbitration and jury trials were significant at the 0.01 level ($6,700 vs. $44,700 for mean cost of error and $1,900 vs. $28,600 for expected cost).

[52]"No decision error" of 25.8 percent in arbitration cases is significantly different at the 0.01 level from "no decision error" in both bench trials (14.8 percent) and jury trials (13.9 percent).

cated driver, for example, may seek compensation for medical expenses already incurred and pain and suffering previously suffered (current damages); the cost of future surgery anticipated by her physician and prospective pain and suffering (future damages); and punitive damages based on the defendant's reckless behavior while driving intoxicated. The damages code is based on plaintiffs' damages *allegations*, not the type of damages ultimately recovered by plaintiffs. Awards generally are not sufficiently allocated by *Verdict Search California* and the adjudicator to consistently determine the type of damages ultimately awarded.

Behavioral economics theory posits that a party is more likely to recover actual losses already sustained ("current" damages) than lost future profits or other relatively remote damages ("future" damages), even when a party is entitled to recover both types of damages.[53] In a breach of contract action against a contractor who abandoned a house construction project, for example, the plaintiff is more likely to recover its advance payment to the contractor than the rental income lost between the original contract completion date and the actual completion date.[54] Although a nonbreaching party is entitled to "the amount which will compensate the party aggrieved for all the detriment proximately caused thereby," that is, the equivalent of the benefits of contract performance,[55] studies show that jurors and judges are reluctant to award both damages actually incurred and damages yet to be sustained.[56]

The study does not appear to substantiate the existence of a cognitive distinction between "current" damages awards and "future" damages awards. As indicated in Table 9, plaintiffs seeking only future damages fared poorly, recovering a net award in only 32.4 percent of the cases. Plaintiffs alleging only current damages prevailed in 45.2 percent of their cases. Plaintiffs seeking both current and future damages recovered a net reward in 47.9 percent of the cases. Although cases alleging current damages claims are associated with higher win rates, the differences between those win rates and

---

[53]See Jonathan Baron, Thinking and Deciding 409–31 (Cambridge University Press 2000).

[54]Facts based on *Henderson v. Oakes-Waterman Builders*, 44 Cal. App. 2d 615 (1941), reversing trial court's determination of damages and holding owner was entitled to recover advance payment, cost of demolition and reconstruction, and loss of rental value.

[55]California Civil Code § 3300.

[56]David Cohen & Jack L. Knetsch. Judicial Choice and Disparities Between Measures of Economic Value, in Choices, Values and Frames, supra, 436–39.

Table 9: Win Rates by Nature of Damages

Damages Claim	*Win Rate*	*# of Cases*
Current only	45.2%	936
Current and punitive damages	56.3%	71
Future only	32.4%	34
Current and future	47.9%	838
Current, future, and punitive damages	71.2%	52

NOTE: Not shown are cases for which it was not possible to identify the nature of the claim (108 cases), and for which a claim for punitive damages was combined with a future damages claim (only four cases).

the win rate for cases alleging only future damages are not statistically significant at the 0.05 level.

Table 10 demonstrates the effects of the damages claim on the parties' decision errors. Compared to cases with only current damages claims (Panel 10a), those with only future damages claims (Panel 10c) exhibited greater decision error and cost of error by both parties. However, the number of cases with only future damages claims was small (34 cases, with defendant decision error in only eight cases). Another way to identify differences is to compare cases with both current and future claims (Panel 10d) with cases having only current claims. The extent of defendant decision error in cases alleging both current and future claims is somewhat greater than in cases with only current claims (26.4 percent vs. 20.4 percent).[57] Plaintiffs' decision error was somewhat lower in cases with both current and future damage claims relative to current claims alone (59.4 percent vs. 64.0 percent), but plaintiffs showed higher mean cost of error and expected cost of error in cases alleging both current and future damages.[58]

Decision error rates were significantly affected by the presence of a punitive damages claim. Defendant decision error in cases with punitive damages claims rose from 20.4 percent in current damages only claims to 36.6 percent in current and punitive damages cases, and from 26.4 percent

---

[57]The difference was significant at the 0.01 level. Defendants' mean cost of error was substantially greater in those cases that also had future claims ($1,641,500 vs. $336,000), as was their expected cost of error ($432,900 vs. $68,600), with both differences being significant at the 0.01 level.

[58]Though relatively modest in degree, the difference in decision error rates is significant at the 0.01 level. Plaintiffs' mean cost of error was substantially greater in those cases that also had future claims ($66,000 vs. $23,900), as was their expected cost of error ($39,200 vs. $15,300), with both differences being significant at the 0.01 level.

Table 10: Decision Error and Cost of Error—By Nature of Damages

	Decision Error					*Cost of Error*	
Error Type	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
Panel 10a: Current Claim Only							
No error	146	15.6%	542.9	734.5	252.4	NA	NA
Plaintiff error	599	64.0%	10.8	370.8	34.8	23.9	15.3
Defendant error	191	20.4%	727.5	391.5	109.4	336.0	68.6
Panel 10b: Current and Punitive Damages Claim							
No error	9	12.7%	336.9	637.8	111.1	NA	NA
Plaintiff error	36	50.7%	0.3	610.3	38.1	37.8	19.2
Defendant error	26	36.6%	1,373.0	454.1	76.8	918.9	336.5
Panel 10c: Future Claim Only							
No error	3	8.8%	1,468.7	5,293.3	333.3	NA	NA
Plaintiff error	23	67.6%	(18.2)	1,999.2	38.6	56.9	38.5
Defendant error	8	23.5%	7,788.1	4,870.0	879.4	2,918.1	686.6
Panel 10d: Current and Future Claim							
No error	119	14.2%	381.9	1,005.1	139.4	NA	NA
Plaintiff error	498	59.4%	2.2	741.1	68.2	66.0	39.2
Defendant error	221	26.4%	2,626.1	984.6	344.2	1,641.5	432.9
Panel 10e: Current, Future, and Punitive Damages Claim							
No error	9	17.3%	279.1	580.0	87.8	NA	NA
Plaintiff error	19	36.5%	3.3	643.8	91.6	88.3	32.3
Defendant error	24	46.2%	4,761.3	1,268.2	115.4	3,493.1	1,612.2

NOTE: Not shown are cases for which it was not possible to identify the nature of the claim (108 cases), and for which a claim for punitive damages was combined with a future damages claim (only four cases).

in current and future damages claims to 46.2 percent in current, future, and punitive damages claims.[59] By contrast, plaintiffs' decision error was lower in cases alleging punitive damages. When a punitive damages claim was joined with a current damages claim, plaintiffs' decision error decreased from 64 percent (current damages only) to 50.7 percent (current and punitive damages). In cases where a punitive damages claim was joined with a current and future damages claim, decision error decreased from 59.4 percent (current and future damages only) to 36.5 percent (current, future, and punitive damages).[60]

The substantially higher defendant error rates in punitive damage claims may be attributable to the difficulty of predicting the amount of punitive damage awards and the defendants' inadequate evaluative adjustments for non-paradigmatic claims. Experimental studies show that individual differences in punitive damage awards "produce severe unpredictability and highly erratic outcomes"; study participants show strong agreement in finding punitive intent, but "there is no consensus about how much in the way of dollars is necessary to produce appropriate suffering in a defendant."[61] (That punitive damages awards are unpredictable is challenged by Theodore Eisenberg's recent empirical study, finding, inter alia, "minimal, though observable, variation in the dispersion of the punitive and compensatory damage ratio over the years [1992–2001] and between trial modes."[62])

---

[59]Both defendant decision error rate differences are significant at the 0.01 level. Though defendants' cost of error also substantially increased in cases with punitive damages claims—with mean cost of error rising from $336,000 (current damages only) to $918,900 (current and punitive damages) and from $1,641,500 (current and future damages only) to $3,493,100 (current, future, and punitive damages claims)—these differences are not significant at the 0.05 level. There were similar dramatic differences in defendants' expected cost of error: $68,600 vs. $336,500 (current vs. current and punitive damages) and $432,900 vs. $1,612,200 (current and future vs. current, future, and punitive damages), with the first not being significant at the 0.05 level but the second being significant at the 0.01 level.

[60]Both plaintiff decision error rate differences are significant (at the 0.05 and 0.01 levels, respectively). None of the differences in mean cost or expected cost of error values in cases with punitive damages cases were significantly different at the 0.05 level from their counterpart cases lacking punitive damages claims.

[61]Cass Sunstein et al., Assessing Punitive Damages (With Notes on Cognition and Valuation in Law), in Sunstein, supra, at 232, 240.

[62]Theodore Eisenberg et al., Juries, Judges, and Punitive Damages: Empirical Analysis Using the Civil Justice Survey of State Courts 1992, 1996, and 2001, 3 J. Empirical Legal Studies 276 (2006).

Whether the amount of punitive damages is predictable or unpredictable, the defendants in our study displayed seriously diminished predictive capacity in punitive damage claims. The defendants' relatively poor outcomes suggest that they either ignore the non-paradigmatic variable (punitive damage claim) or erroneously draw problem-solving analogies between the unexceptional cases (no punitive damage claim) and the exceptional case (punitive damage claims). The risk of this type of decision-making error ("negative problem solving transfer") is high when cases appear superficially similar: surface similarity in story line, causes, context, and phrasing frequently leads decision makers to "retrieve and apply a solution to a nonanalogous problem (negative transfer) and thereby waste their cognitive resources or arrive at an erroneous solution."[63]

C. Decision Error and its Costs—Analysis of Attorney-Mediator Sample

Although the primary data set includes 5,116 attorneys—about 20 percent of all California litigation attorneys—and the decision error rates are remarkably consistent with other study results, one may question whether the attorneys in the data set have singular risk-taking propensities that impeded a negotiated settlement and ultimately resulted in significant decision errors. This question cannot be resolved empirically because we will never be able to compare the study decision error rates with decision error rates for cases that were settled; the settled cases do not yield a benchmark trial or arbitration award against which we could compare the negotiated settlement amount. However, we can very roughly probe for selection bias, that is, whether our arguably overconfident study attorneys exhibit higher decision error rates than attorneys with substantial, publicly recognized skills and experience in settling cases.

To identify attorneys with substantial settlement experience and dispute resolution skills, we reviewed lists of 939 California mediators either serving on Superior Court mediator panels, affiliated with private dispute resolution companies, or currently a member of the Southern California Mediation Association. We then searched each mediator's name in Verdict Search, limiting the search to California cases reported between 1985 and 2006, to determine whether the mediator had represented a plaintiff or defendant in a case tried through verdict or arbitration award. (Not all the

---

[63]M. Bassok, Analogical Transfer in Problem Solving, in The Psychology of Problem Solving 343 (J.E. Davidson & R.J. Sternberg, eds., Cambridge University Press 2003).

939 mediators were necessarily litigation attorneys at any time during that period, since the courts' lists include some non-attorneys, former judges, and non-litigation attorneys.) The search yielded 672 cases reported during the 1985–2006 period, of which 369 met the case-selection criteria used for the primary study data set; of the remaining 303 cases, 150 were settled and 153 did not meet the selection criteria for other reasons.[64]

The presence of an attorney-mediator generally was associated with a reduced decision error rate.[65] Table 11, Panel 11a summarizes the experience for 369 cases in which one of the parties was represented by an attorney-mediator. Total decision error in this sample is less relative to the primary sample presented in Table 1; "no error" in attorney-mediator cases is 21.1 percent relative to 14.5 percent in the primary sample.[66]

In cases where plaintiffs were represented by an attorney-mediator, summarized in Table 11, Panel 11b, plaintiffs' decision error is lower than the primary sample (48.5 percent relative to 61.2 percent), although defendants' decision error is higher (32.0 percent relative to 24.3 percent).[67] Nonetheless, the total amount of decision error is lower for the plaintiff attorney/mediator sample than the primary sample; "no error" is 19.5 percent relative to 14.5 percent.[68]

Similarly, in cases where defendants were represented by an attorney-mediator, summarized in Table 11, Panel 11c, defendants' decision error is lower than the primary sample (21.5 percent relative to 24.3 percent).

---

[64]The attorney-mediator data set spans a 21-year period (1985–2006), whereas the primary study data set covers a 38-month period (November 2002–December 2005). Whether a party is represented by an attorney who also serves as a mediator is not a fact separately reported in VerdictSearch and hence was not a variable coded in the primary study data set.

[65]Rachlinski suggested that framing effects might be mitigated by the intervention of attorneys who were more understanding of framing biases: "The framing theory suggests another positive influence attorneys may have in reducing the costs of litigation. An attorney may have some power to reframe a settlement offer, sparing the client the most costly aspects of framing . . . Thus, the framing model of litigation poses a powerful role for the attorney. The attorney can control the client's frame, thereby influencing settlement decisions in either direction." Rachlinski (1996), supra, at 171–72. See Russell Korobkin & Chris Guthrie, Psychology, Economics and Settlement: A New Look at the Role of the Lawyer, 76 Tex. L. Rev. 77 (1997).

[66]The difference is significant at the 0.01 level.

[67]The two differences are significant at the 0.01 level and 0.05 level, respectively.

[68]This difference is not significant at the 0.05 level, having a p value of 0.11.

Table 11: Decision Error and Cost of Error—Attorney-Mediator Sample

	Decision Error					*Cost of Error*	
Error Type	*# of Cases*	*% of Cases*	*Mean Award ($1,000s)*	*Mean Demand ($1,000s)*	*Mean Offer ($1,000s)*	*Mean Cost of Error ($1,000s)*	*Expected Cost of Error ($1,000s)*
Panel 11a: All Cases							
No error	78	21.1%	348.7	567.9	90.4	NA	NA
Plaintiff error	194	52.6%	12.8	558.8	61.2	48.4	25.5
Defendant error	97	26.3%	1,570.8	670.8	217.4	900.0	236.6
Panel 11b: Attorney-Mediator Represents Plaintiff							
No error	33	19.5%	512.4	702.4	143.0	NA	NA
Plaintiff error	82	48.5%	18.4	820.6	86.7	68.4	33.2
Defendant error	54	32.0%	1,615.2	706.6	218.3	908.6	290.3
Panel 11c: Attorney-Mediator Represents Defendant							
No error	45	22.5%	228.7	469.2	51.9	NA	NA
Plaintiff error	112	56.0%	8.7	367.1	42.5	33.8	18.9
Defendant error	43	21.5%	1,515.0	625.8	216.2	889.2	191.2

Interestingly, in these attorney-mediator cases, plaintiffs' decision error is also lower (56.0 percent relative to 61.2 percent). Thus for both conditions of reduced error, total decision error is lower in these cases; "no error" is 22.5 percent relative to 14.5 percent in the primary sample.[69]

Regardless of which party is represented by an attorney-mediator, the total amount of error is modestly lower. Much less can be concluded from an examination of the mean cost of error due to the construction of the attorney-mediator sample. That sample covers a much longer time period than the primary data set (21 years vs. 38 months), rendering many of the values non-comparable with the primary sample used in Table 1. This is an area worthy of continued research.

We also examined specific case types to assess the incidence of decision error in the attorney-mediator cases. Because the sample of attorney-mediator cases, when classified by case type and whether the mediator represented a plaintiff or a defendant, was small compared to the primary data set, we focused on personal injury cases, the most common type of cases in the primary sample. Consistent with the overall findings of reduced decision error in attorney-mediator cases, we found that personal injury cases in which the parties were represented by attorney-mediators showed a lower decision error rate than those in the primary sample. Plaintiffs' decision error rate in personal injury cases was 45.2 percent in the attorney-mediator sample and 53.2 percent in the primary sample. Defendants' decision error rate in personal injury cases showed a similar pattern—16.8 percent in the attorney-mediator sample and 26.3 percent in the primary sample.

V. Conclusion

Because each case in the study requires a settlement decision by both a plaintiff and a defendant, this study tests 9,064 decisions—2,054 cases and 4,108 decisions in the 2002–2005 primary set, 1,806 cases and 3,612 decisions in the 1964–2004 historical set, and 672 cases and 1,344 decisions in the 1985–2006 attorney/mediator set. Plaintiffs erroneously concluded that trial was a superior option in 61.2 percent of the primary set cases, while defen-

---

[69]Though the changes in defendants' and plaintiffs' decision error are not significant at the 0.05 level, the difference in "no decision error" (22.5 percent vs. 14.5 percent) is significant at the 0.01 level.

dants made an erroneous assessment in 24.3 percent of those cases. The magnitude of defendants' errors, however, vastly exceeded that of plaintiffs' errors. The historical review of attorney/litigant decision making indicates that the incidence of decision error increased moderately, while the magnitude of decision error increased dramatically. The attorney/mediator cases show comparatively low decision error rates that nevertheless would be unacceptable in other high-skill domains like medicine, aeronautics, or structural engineering. If Gross and Syverud are correct in asserting the "real question for any party is whether it would have been better off if it had not gone to trial," the answer for a clear majority of plaintiffs and one-quarter of defendants is "Yes."[70]

From the remarkably consistent decision error rates shown in this study and three prior studies, a renewed emphasis on reducing attorney/litigant decision-making error could emerge. Further research can identify and perhaps eliminate conditions and framing biases associated with high decision error rates while identifying and replicating the conditions and decision-making practices associated with low decision error rates. The lower decision error rates correlated with a party's service of a 998 offer, for instance, may indicate that a party serving a 998 offer undergoes a beneficial evaluative process that results in improved decision making. The attorney-mediator data, moreover, suggest that attorneys trained and experienced in dispute resolution, and perhaps more cognizant of framing biases, may have a salutary effect on attorney/litigant decision making. An attorney-mediator's representation of a plaintiff is associated with a 21 percent reduction in plaintiff decision error, and the presence of an attorney-mediator representing any party is correlated with a dramatic reduction in the overall incidence of decision error, the percentage of "no error" cases rising from 14.5 percent in the primary sample to 21.1 percent in the attorney-mediator sample.

In his recent book, *Expert Political Judgment*, Philip Tetlock tests political predictions by 284 experts, finding that their probability assessments frequently are inaccurate. Explaining the motivation for the study, he states: "We can draw cumulative lessons from experience only if we are aware of gaps between what we expected and what happened, acknowledge the possibility that those gaps signal shortcomings in our understanding, and test alternative interpretations of those gaps in an evenhanded fashion." This

---

[70]Gross & Syverud (1996), supra, at 41.

study hopefully fulfills similar objectives, illuminating gaps between expectations and results, promoting a candid and objective assessment of predictive shortcomings, and presenting data and interpretations to improve attorney/litigant decision making and, eventually, "close the gap between what they said would happen and what subsequently did happen."[71]

Appendix: Likelihood Ratio Tests

Variable Class	*# of Parameters*	*Degrees of Freedom*	*L-R Chi Square*	p *Value*
Plaintiff	6	12	14.6427	0.2616
Defendant	8	16	24.4649	0.0798
Plaintiff attorney gender	4	8	25.7011	0.0012
Plaintiff attorney firm size	1	2	1.9513	0.3769
Plaintiff attorney experience	10	20	38.1059	0.0086
Plaintiff attorney school academic rank	1	2	7.0855	0.0289
Plaintiff attorney school diversity rank	1	2	0.2760	0.8711
Defendant attorney gender	4	8	12.4398	0.1326
Defendant attorney firm size	1	2	0.2693	0.8740
Defendant attorney experience	9	18	31.5934	0.0246
Defendant attorney school academic rank	1	2	0.0953	0.9535
Defendant attorney school diversity rank	1	2	5.8111	0.0547
Case type	12	24	204.3922	0.0000
Nature of damages	3	6	29.7042	0.0000
Nature of alleged wrong	2	4	6.0450	0.1958
Forum	3	6	75.0184	0.0000
Insurance	1	2	1.6174	0.4454
998 offer	2	4	163.6942	0.0000
Alternative dispute resolution	2	4	5.6822	0.2242

[71]Philip Tetlock, Expert Political Judgment 235, 238, n.22 (Princeton University Press 2005).

Link to the ABA Model Rules:

https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents/

Link to California Rules of Professional conduct

http://www.calbar.ca.gov/Attorneys/Conduct-Discipline/Rules/Rules-of-Professional-Conduct/Current-Rules

CIVIL CODE - CIV

DIVISION 3. OBLIGATIONS [1427 - 3273] *(Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.)*

PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273] *(Part 4 enacted 1872.)*

TITLE 1.81. CUSTOMER RECORDS [1798.80 - 1798.84] *(Title 1.81 added by Stats. 2000, Ch. 1039, Sec. 1.)*

1798.81.5. (a) (1) It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.

(2) For the purpose of this section, the terms "own" and "license" include personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates. The term "maintain" includes personal information that a business maintains but does not own or license.

(b) A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(c) A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party that is not subject to subdivision (b) shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Personal information" means either of the following:

(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.

(ii) Driver's license number or California identification card number.

(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(iv) Medical information.

(v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account.

(2) "Medical information" means any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional.

(3) "Health insurance information" means an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(e) The provisions of this section do not apply to any of the following:

(1) A provider of health care, health care service plan, or contractor regulated by the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1).

(2) A financial institution as defined in Section 4052 of the Financial Code and subject to the California Financial Information Privacy Act (Division 1.2 (commencing with Section 4050) of the Financial Code).

(3) A covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Availability Act of 1996 (HIPAA).

(4) An entity that obtains information under an agreement pursuant to Article 3 (commencing with Section 1800) of Chapter 1 of Division 2 of the Vehicle Code and is subject to the confidentiality requirements of the Vehicle Code.

(5) A business that is regulated by state or federal law providing greater protection to personal information than that provided by this section in regard to the subjects addressed by this section. Compliance with that state or federal law shall be deemed compliance with this section with regard to those subjects. This paragraph does not relieve a business from a duty to comply with any other requirements of other state and federal law regarding the protection and privacy of personal information.

(Amended by Stats. 2015, Ch. 96, Sec. 1. (AB 1541) Effective January 1, 2016.)

Legal Trends Report

By Clio

2019

Table of contents

Introduction

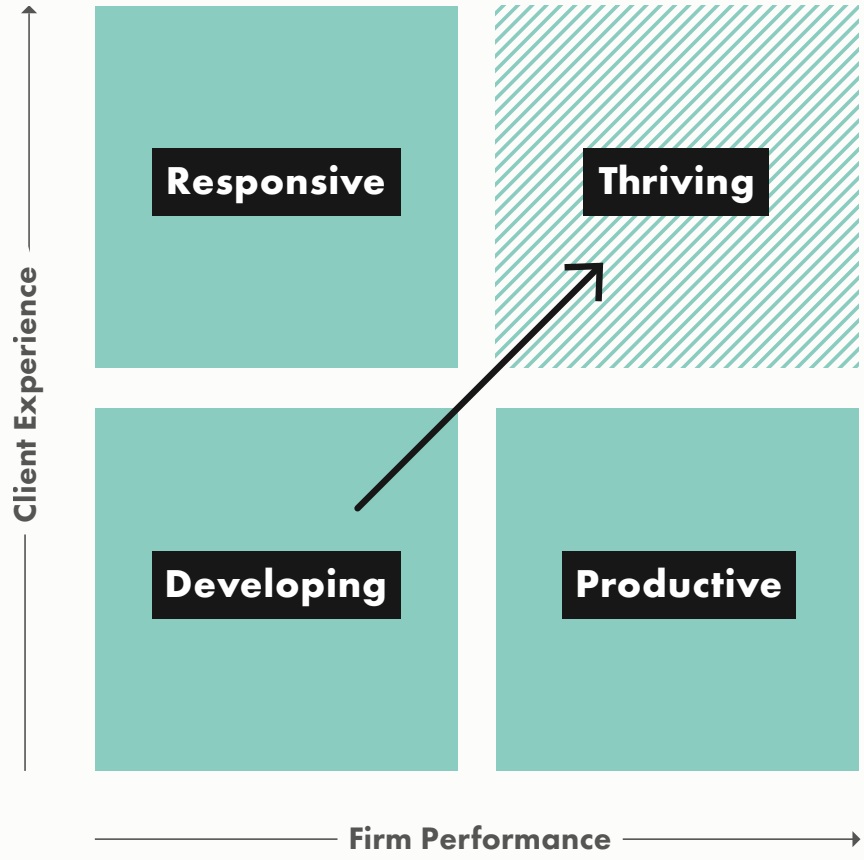
Closing the gap

The market for legal services faces a critical paradox. On one hand, the vast majority of law firms say they want to increase their revenues, yet they have trouble finding business. On the other, clients struggle to get help with their legal problems.

This paradox represents a market gap that shouldn't exist—and one that presents an enormous opportunity for firms that can build a strong business approach for their legal practice.

Many high-growth firms are getting it right. We call these "thriving" firms because they've been able to achieve substantial year-over-year revenue growth that is both consistent and predictable. We believe these firms have achieved high growth over a sustained period of time due to two critical factors: a focus on client experience and firm efficiency. We've illustrated this growth path in a new format: the Law Firm Maturity Model.

Law Firm Maturity Model



In the bottom-left quadrant are new firms or firms that have either struggled or have yet to achieve the success they want. Firms that progress along the client-experience axis are those that become responsive to client needs. These are the firms that know how to attract new business and earn strong satisfaction among their clients. Firms that progress along the firm-performance axis put more time toward revenue-generating tasks for clients, while keeping overhead costs low and investing in productivity initiatives. Thriving firms progress along both axes. These firms consistently increase the amount of business they bring in while capturing the full value from all of the client-facing, revenue-generating work they perform.

We can learn a lot from high-growth firms—and we believe more law firms should. Not only are these firms achieving major success in the form of rapidly expanding revenues, they're doing it while closing the market gap and delivering more legal services to the clients who need them.

In the pages that follow, we've created the most extensive, in-depth analysis on how lawyers can drive new business and achieve greater success for their firms.

Thriving firms achieve predictable, high growth over time

New this year

Since 2016, the *Legal Trends Report* has uncovered the most groundbreaking insights into the business of legal practice in the 21st century. Now in its fourth year of publication, we've expanded the scope of our research to include new approaches to understanding some of the most pressing realities that lawyers—and their clients—face today.

Determining what drives law firm success

We conducted the first-ever longitudinal data analysis to determine how thriving firms achieve consistent, long-term growth in revenue over time, and what distinguishes them from firms that haven't seen any growth or have shrunk over the same period. By comparing growing, stable, and shrinking firms over a five-year period, we're able to show how key performance metrics impact success.

What clients really look for when hiring a lawyer

We surveyed consumers to shed more light on how they look for a lawyer, what they expect when reaching out, and what drives them away. Our findings show that referrals aren't the only means clients use to seek a lawyer, and that clients have a high bar for deciding who to reach out to—and who to ultimately hire.

Putting law firm responsiveness to the test

What's it like shopping for a lawyer in 2019? To answer this, we emailed 1,000 law firms, and phoned 500 from the same group, to determine just how prepared lawyers are to earn the business of potential clients when they reach out. In doing so, we've collected the largest primary data set on law firm responsiveness —which puts a spotlight on key opportunities for law firms to be truly competitive in acquiring new clients.

Data sources included in the *2019 Legal Trends Report*

We use a range of methodologies and data sources to build a comprehensive understanding of how lawyers run their firms in today's market for legal services. This year, we've expanded the scope of our data sources even further to uncover new insights unlike any before.

Clio data

The *Legal Trends Report* uses aggregated and anonymized data from tens of thousands of legal professionals in the United States. This includes data from January 1, 2013 to December 31, 2017, which was used to conduct our longitudinal analysis of law firm success. In reviewing actual usage data, we identify large-scale industry trends that would otherwise be invisible to law firms.

Law firm survey

We surveyed 2,507 legal professionals, representing both Clio users and non-Clio users. By assessing the existing needs and strategies of law firms, we're able to better align our data analyses with real law firm goals.

Consumer survey

We surveyed 2,000 consumers to understand what they look for when searching for professional legal services and what types of experiences they expect. Our sample was representative across all adult age groups, genders, and geographic regions in the United States.

Email and phone outreach

We emailed a random sample of 1,000 law firms in the United States, and then phoned 500 of these firms, to assess responsiveness and quality of service. Our sample had equal representation across five practice areas, including Family, Criminal, Bankruptcy, Business Formation, and Employment, and comprised firms of all sizes.

Aggregated and anonymized data from tens of thousands of legal professionals

2,507 legal professionals surveyed

2,000 consumers surveyed

1,000 law firms emailed for legal services

500 law firms phoned for legal services

Part 1

This is what law firm growth looks like

For the first time, we've significantly expanded the scope of our data analysis to look at longitudinal, multi-year trends.

Over the last 11 years, Clio has established itself as the system of record for the legal profession, benchmarking key business insights across tens of thousands of law firms—which we've reported in the *Legal Trends Report* for the past four years. Now, in formulating the industry's first longitudinal research, we've further validated the critical business metrics that ultimately contribute to law firm growth.

Through this analysis, we illustrate how thriving law firms increase their revenues more and more over time —and why struggling firms see their revenues decline. From the data in this section, we discuss how critical business inputs contribute to exceptional, long-term growth in firm revenue—serving as a roadmap for any law firm to follow.

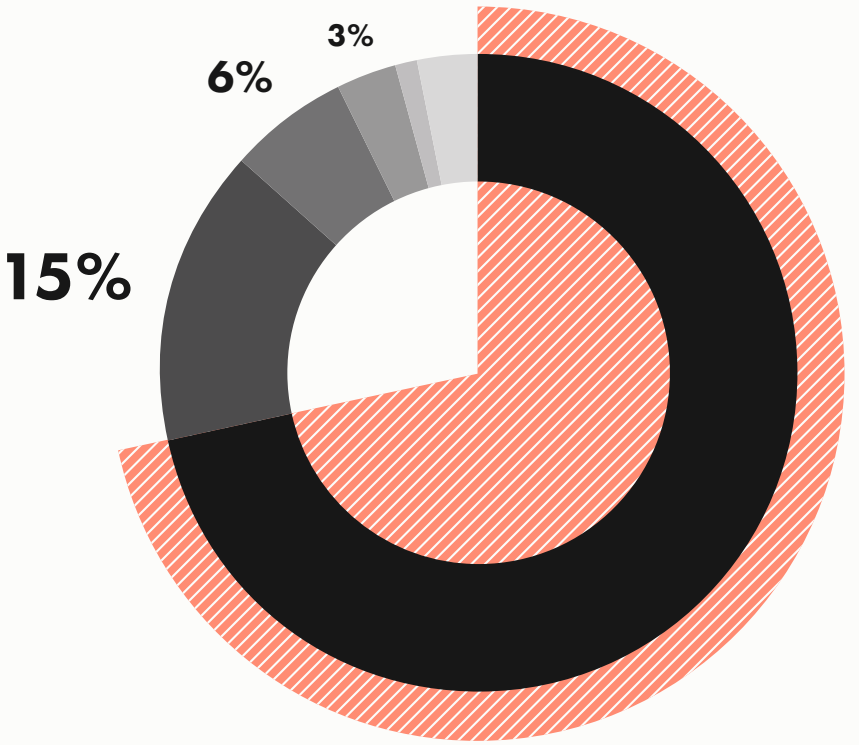
Building our analysis

To better understand what distinguishes thriving law firms from others, we leveraged aggregated and anonymized data from thousands of law firms to design a comparative analysis that zeroed in on three distinct groups defined by their total revenue growth between 2013 and 2017:

- **Growing firms.** Firms that grew their revenues by **at least 20% over five years**.
- **Stable firms.** Firms that neither grew nor declined by **more than 20% over five years**.
- **Shrinking firms.** Firms that saw their revenues decline by **at least 20% over five years**.

Why did we focus on revenue? Aside from being an objective and quantitative benchmark for success, **71%** of lawyers say they consider revenue their most important indicator for law firm growth. Revenue is also a standard measure for the overall health of a business—from small private entities to the very largest—and is a key output for the other business metrics that we compare.

Lawyers ranking revenue as an indicator of growth



71%

Ranked revenue as the most important indicator of growth

Refer to **page 40** for detailed analysis on other indicators.

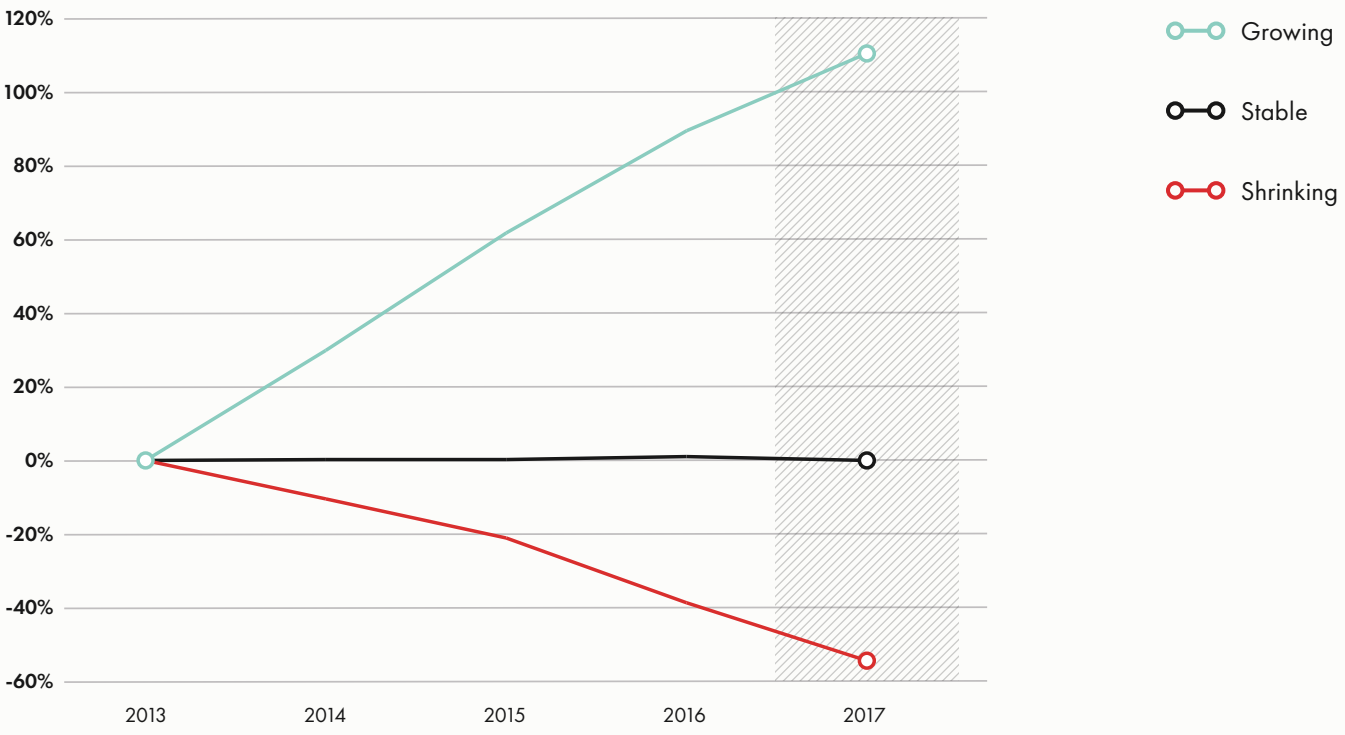
Growing firms grew 20% to 30% year over year

When looking at the total increase in revenues, we determined that growing firms actually grew by **20%** to **30%** year over year to achieve an average of **112%** growth between 2013 and 2017—making them a prime example of the thriving firms described within the Law Firm Maturity Model (see **page 4**).

On the other hand, shrinking firms saw their revenues decrease by **54%**, meaning they took in less than half the revenue in 2017 as they did in 2013. Stable firms maintained approximately the same level of revenue over the same period.

Each group has their own distinct patterns for growth—and these trends stayed consistent even when we controlled for firm size and practice area.

Revenue growth



Shrinking firms saw revenues decline by more than 50%

More lawyers and clients explain part of revenue growth

So what drives growth? The first two metrics we looked at were the average number of lawyers within each firm and the overall number of cases and matters worked among growing, stable, and shrinking firms.

At the start of our analysis, we expected that total revenue earnings would correlate strongly between the number of lawyers hired and the number of clients and matters worked. For example, if a firm were to double the number of lawyers at the firm, it would follow that the firm's capacity for work would also double. Similarly, if that firm worked twice the number of cases, they would essentially double their earnings.

It turned out this wasn't exactly the case. In fact, growing firms took on proportionately more cases and clients relative to the number of lawyers they brought on. While growing firms increased their number of lawyers by **32%** over five years, the number of cases they worked increased by an impressive **57%**.

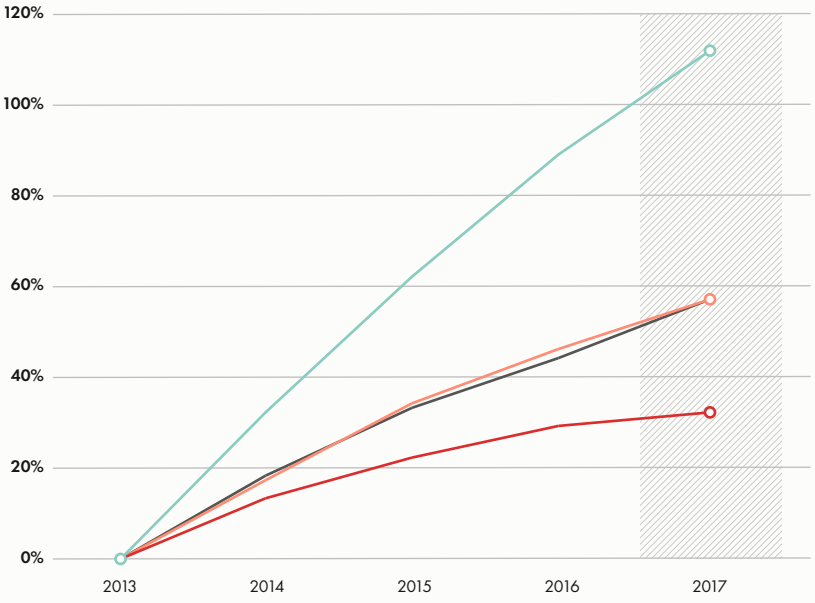
The same goes for the gravity-defying revenue growth among these firms, which saw their total revenues jump by **over 100%**. To put this in perspective, revenue growth for these firms increased at three times the rate at which they brought on new lawyers, and casework increased at twice the rate.

In other words, these firms increased the number of clients they worked with while also increasing the amount of revenue collected from the work they performed. Meanwhile, shrinking firms saw the reverse compounding effect. These firms reduced the number of lawyers they had by **17%** and reduced their total number of cases by **40%**, resulting in a drop in revenue of **54%**.

While revenue growth correlated with an increase in the number of lawyers and cases worked by each firm, this growth was vastly disproportionate, which indicates that other factors are contributing to the success of these growing firms—and which may also explain the negative performance of shrinking firms.

Comparing revenue growth to clients, matters, and lawyers

Growing firms



122% Revenue growth

57% Client growth

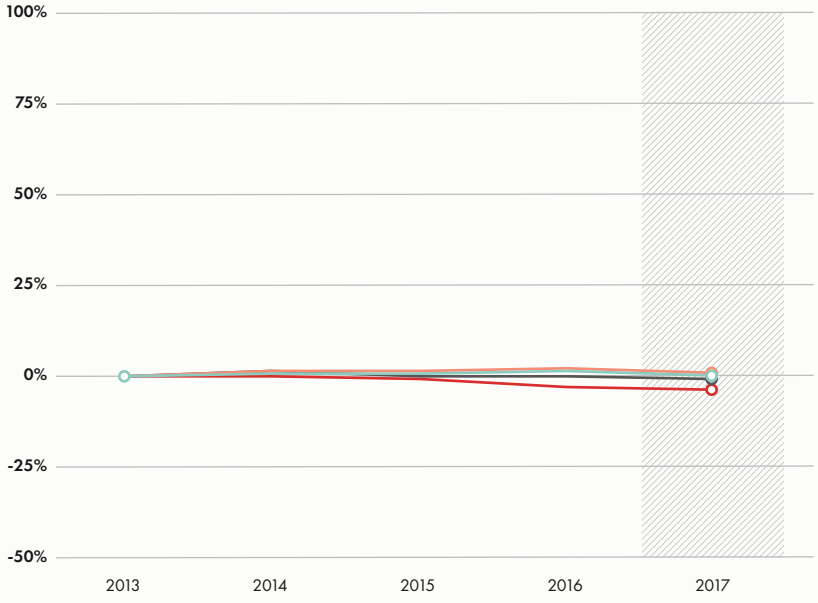
57% Matter growth

32% Lawyer growth

Revenue
Clients
Matters
Lawyers

Growing firms took on increasingly more cases and clients

Stable firms



0% Revenue growth

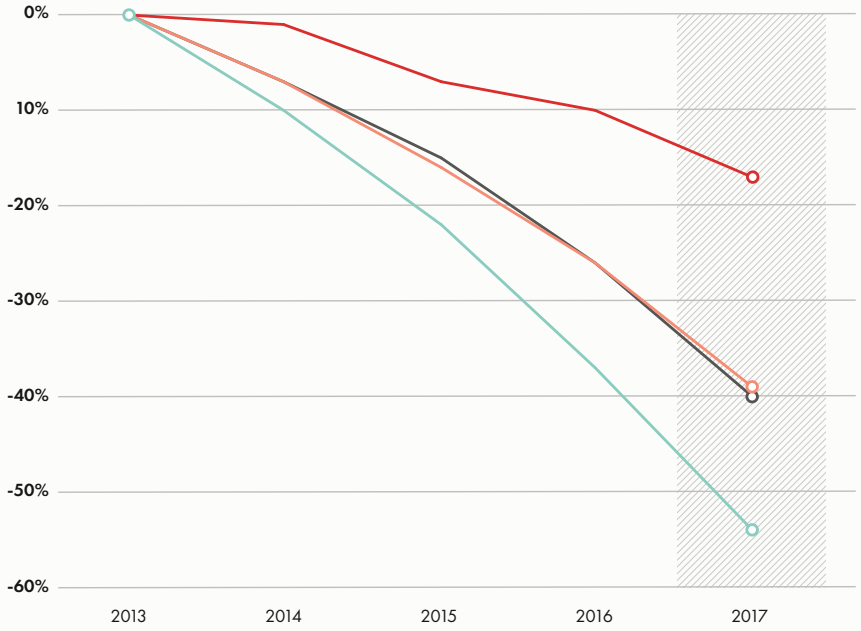
1% Client growth

-1% Matter decline

-5% Lawyer decline

Revenue
Clients
Matters
Lawyers

Shrinking firms



-54%
Revenue decline

-39%
Client decline

-40%
Matter decline

-17%
Lawyer decline

Revenue
Clients
Matters
Lawyers

The power of utilization

Since first publishing the *Legal Trends Report* in 2016, we've benchmarked several critical business metrics for the legal industry, which include utilization, realization, and collection rates. These metrics are discussed in more detail—and with updated figures for 2019—in Section 6 of this report. These critical business metrics also make up a significant portion of our analysis of growing and shrinking law firms.

Utilization rates turned out to be a key driver for revenue growth among growing firms.

- Utilization is a measure of how many hours a lawyer puts toward billable work on a given day.

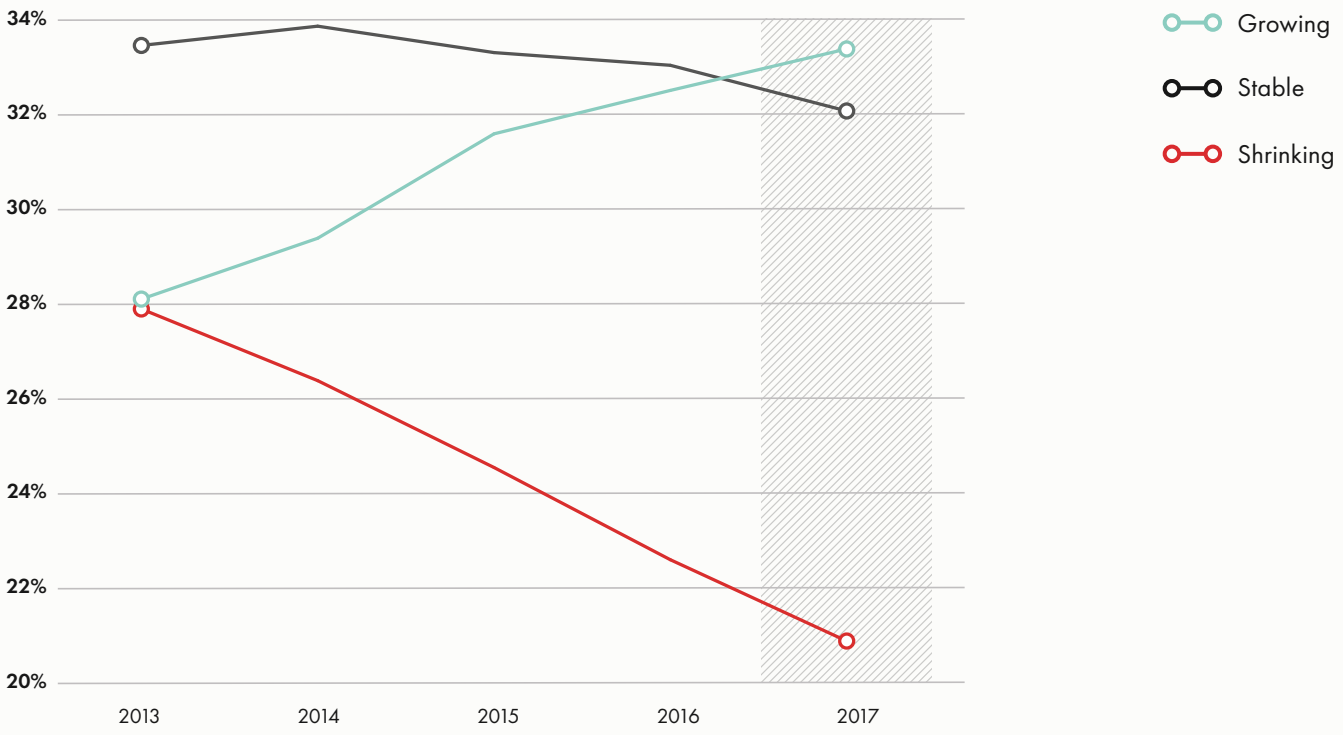
The average utilization rate for law firms this year was **31%**, which means the average lawyer spent only **2.5** hours on billable work each day—a trend that's stayed relatively consistent over the last four years of reporting.

When looking at individual cohorts, we see that stable firms have the highest rate of utilization compared to early data from growing and shrinking firms. Over time, however, growing firms increase utilization rates to 33%, surpassing stable firms. Meanwhile, the opposite is true for shrinking firms, which see utilization rates steadily decline each year, falling from **28% to 21%**.

The impact of utilization on firm revenue can't be understated. High utilization rates indicate that firms are able to bring in more business, and that lawyers are more focused on performing billable work. Boosting productivity per lawyer was at least as important as adding more lawyers to the firm.

Growing firms therefore have the highest earning potential, while shrinking firms struggle to build their revenue opportunities. To put this into perspective, the difference between 21% and 33% utilization is 12% of a day, which equals about a full hour's work—or five hours every week. Compound that difference week after week, for every lawyer at the firm, and it's clear why growing firms are in a much better earning position than shrinking and even stable firms.

Utilization



Thriving firms achieve predictable, high growth over time

Growing firms get more out of their work

Realization and collection rates are two other key business metrics we looked at, both of which show major divergence between growing and shrinking firms:

- **Realization** measures the amount that a firm invoices compared to the amount of billable work performed.
- **Collection** measures the amount that a firm collects compared to the amount invoiced.

Both of these are critical metrics for business performance, as they assess how much value a firm brings in based on the amount of work performed. If realization and collection are high, it means that firms are getting the full value of the work performed.

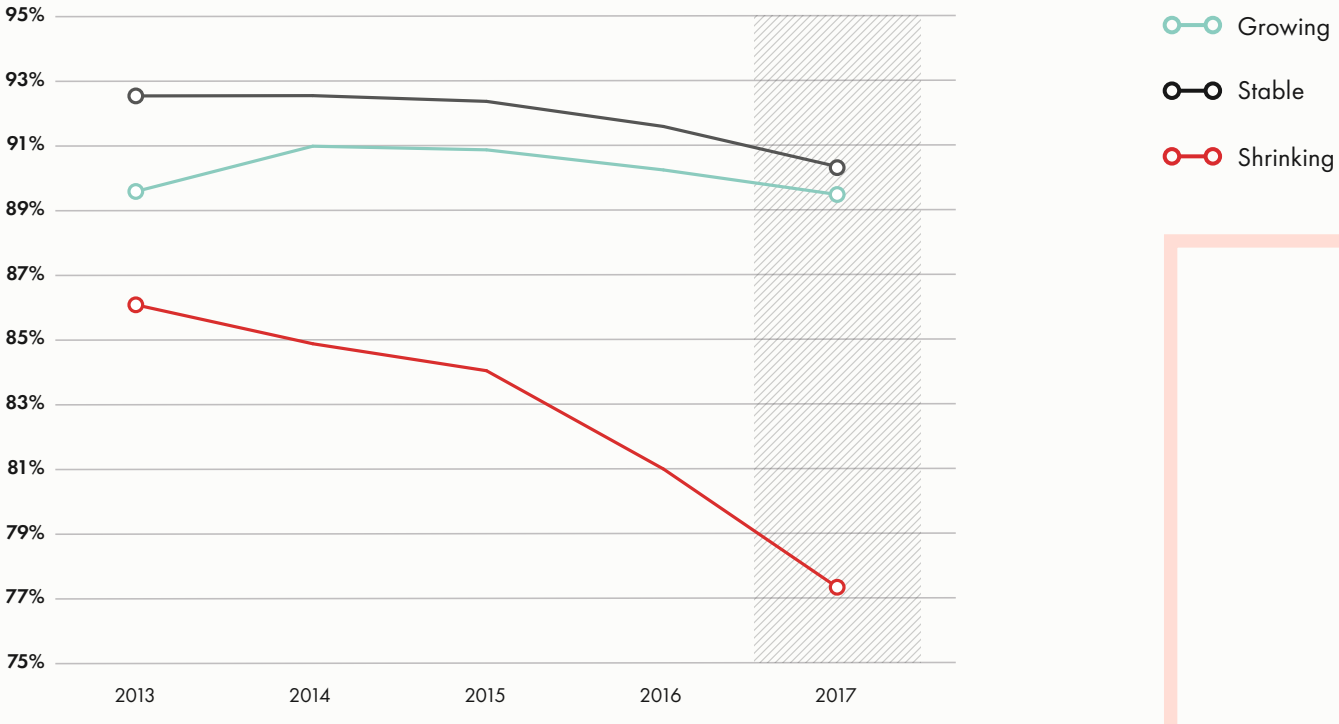
Growing firms start out with **90%** realization, while shrinking firms start at a lower realization of **86%**, which steadily declines to a shockingly low **77%** over time. This means that shrinking firms increasingly don't charge for the work they do.

Stable firms show the highest realization of all three groups, reaching as high as **92%**. This indicates that growing firms are more likely to conduct billable work that never actually gets invoiced when compared to stable firms—though, both maintain high realization above approximately **90%** at all times.

When it comes to collecting payments from clients, growing firms track nearly identically with stable firms, and both maintain higher collection rates above **90%** at all times. Shrinking firms, on the other hand, see drastically diminishing collection rates to **81%** over time. This suggests either they don't have proficient processes in place for collecting payments reliably, or they aren't able to find the types of clients that are more likely to pay them.

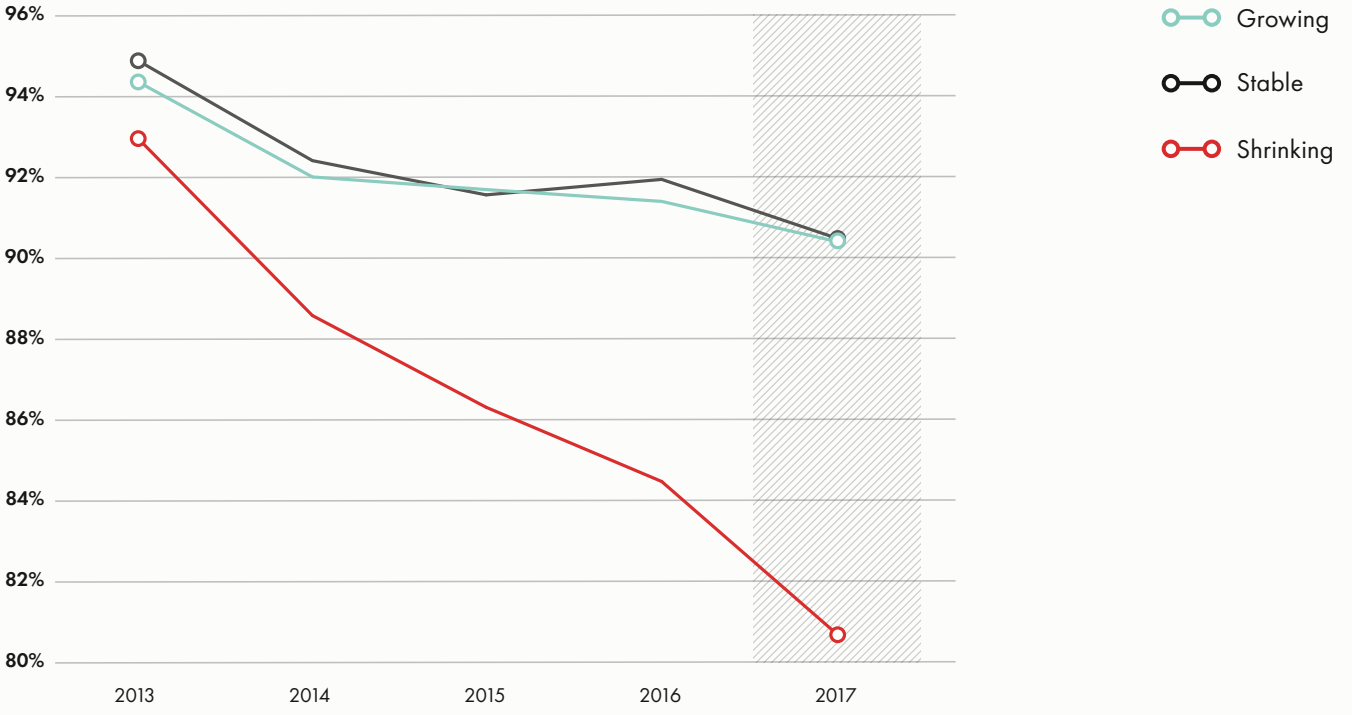
The result on overall business revenues is that shrinking firms earn increasingly less over time from the work they perform, while growing and stable firms are able to maintain relatively high earnings for every hour worked.

Realization



Shrinking firms fail to charge for the work they do at an accelerating rate

Collection

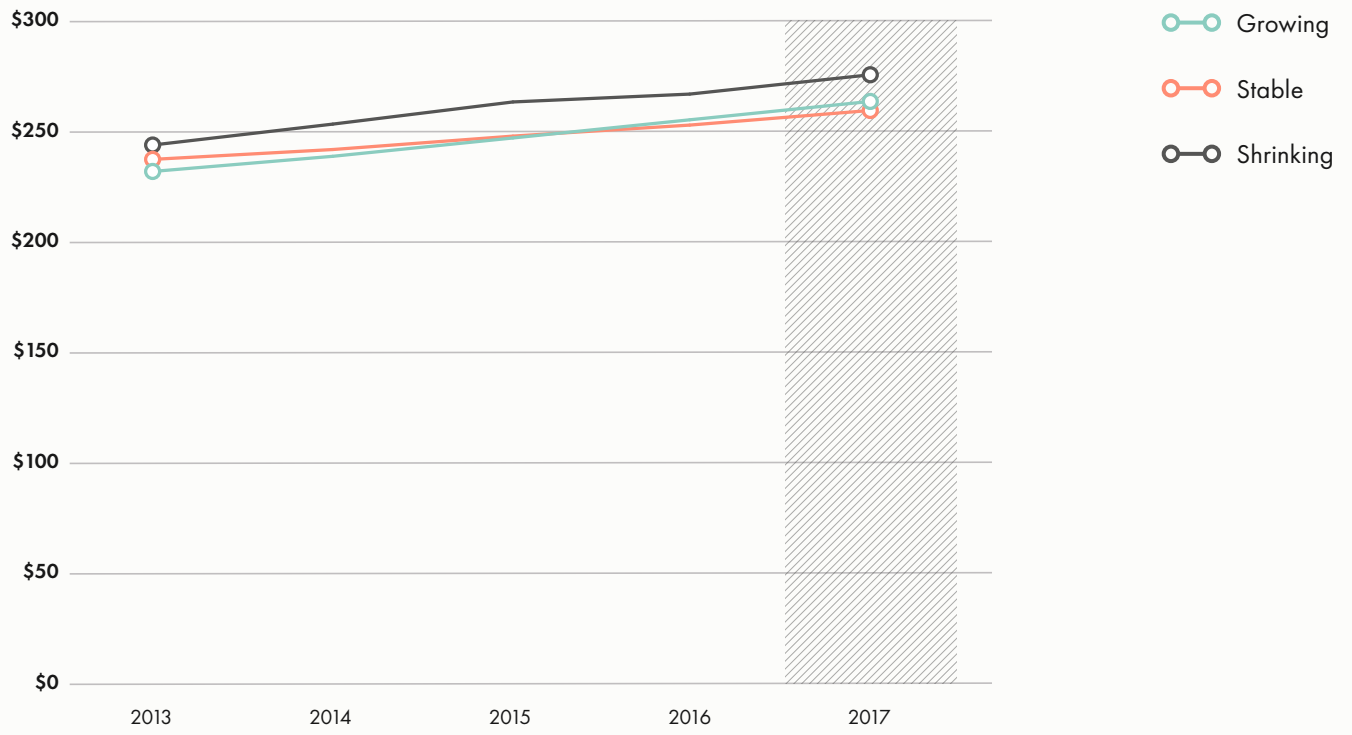


Factors not associated with growth

We compared the results from this analysis across different types of law firms to determine whether factors such as practice area or firm size would yield unique trends, but the data followed similar trajectories—and any dissimilarities were minimal.

Average hourly rates were another factor that we compared. We wanted to see if firms that grow their revenues increased their hourly rates at a higher rate than others, but this wasn't the case. When comparing hourly rates across each group, all three followed a very similar trend in line with the data outlined in the Billable Hour Index, which is discussed in detail in Section 6.

Average hourly rates



What does this mean for lawyers?

It's clear that there isn't one specific factor that defines the type of substantial increase in revenue that we see in growing firms. And, in fact, simply increasing hourly rates—which might seem like an obvious strategy—is not effective in driving long-term growth. Instead, real growth is a result of two factors:

- **Generating more business.** Growing firms increase the amount of work they bring in compared to the number of lawyers they have.
- **Strong business metrics.** Growing firms improve utilization rates over time while maintaining high realization and collection rates.

In other words, growing firms know how to bring in more business while also increasing the capacity of their lawyers to do more work and collect more revenue for every case and client they bring in. Both of these factors align with the firm-performance axis of the Law Firm Maturity Model, outlining a critical measure for how firms should focus their business strategies for success. The sections that follow illustrate key factors that contribute to better client experiences.

Part 2

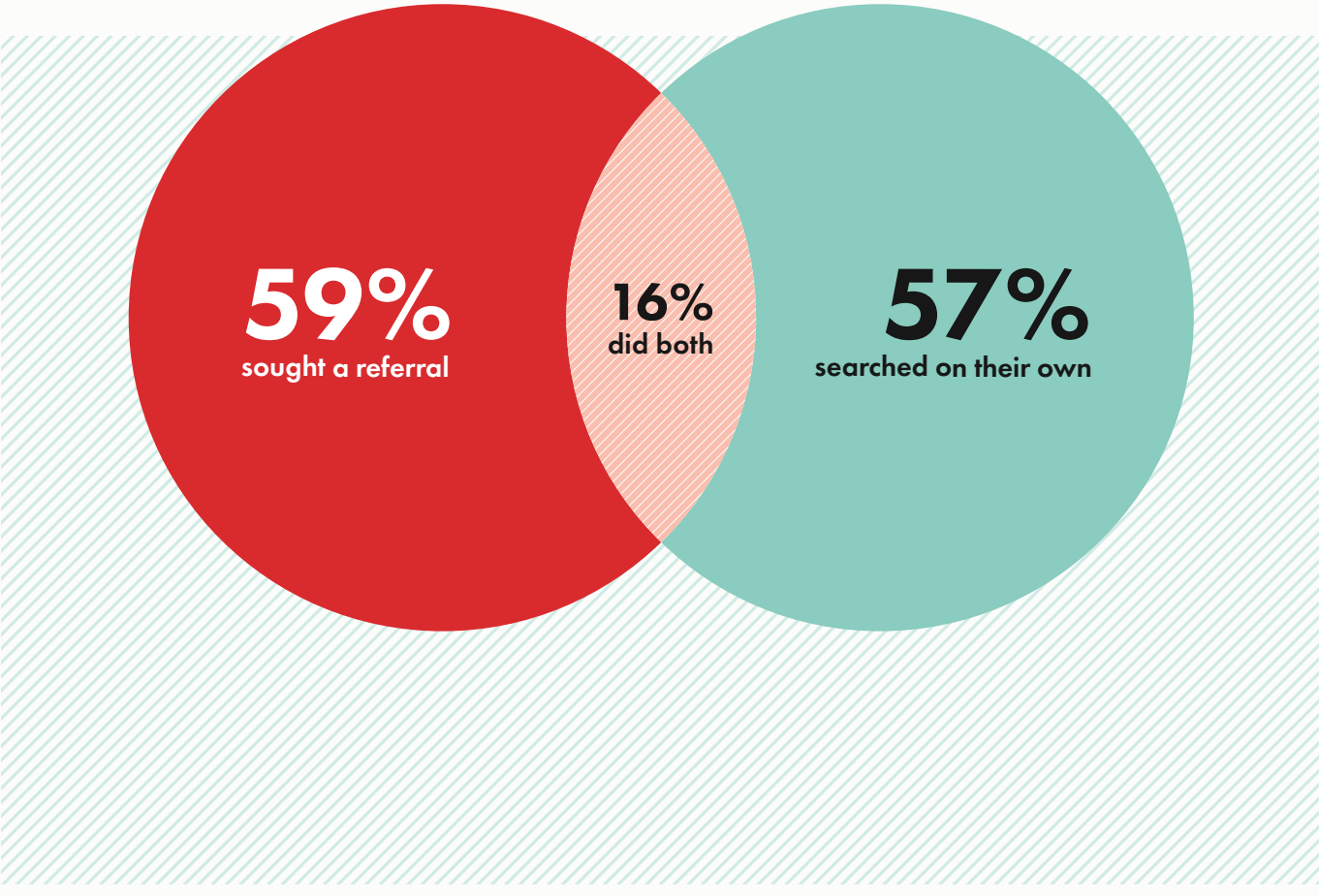
Clients want more than just referrals

In Section 1 of this report, we determined that growing firms know how to consistently bring in new business. A critical component to bringing in new business is to understand how today's client looks for a lawyer.

But what are potential clients really looking for when seeking legal help? To find out, we surveyed 2,000 consumers to learn how clients ultimately choose one lawyer over another. One of the most interesting things we learned is that—despite being recognized as the primary driver for new business—not all clients rely on referrals to find a lawyer. In fact, many opt to search on their own.

When comparing these methods of looking for a lawyer, **59%** of clients sought a referral from someone they know or have been in contact with, but **57%** searched on their own through some other means—and **16%** did both.

Clients seeking a referral versus searching on their own



How clients shop for a lawyer

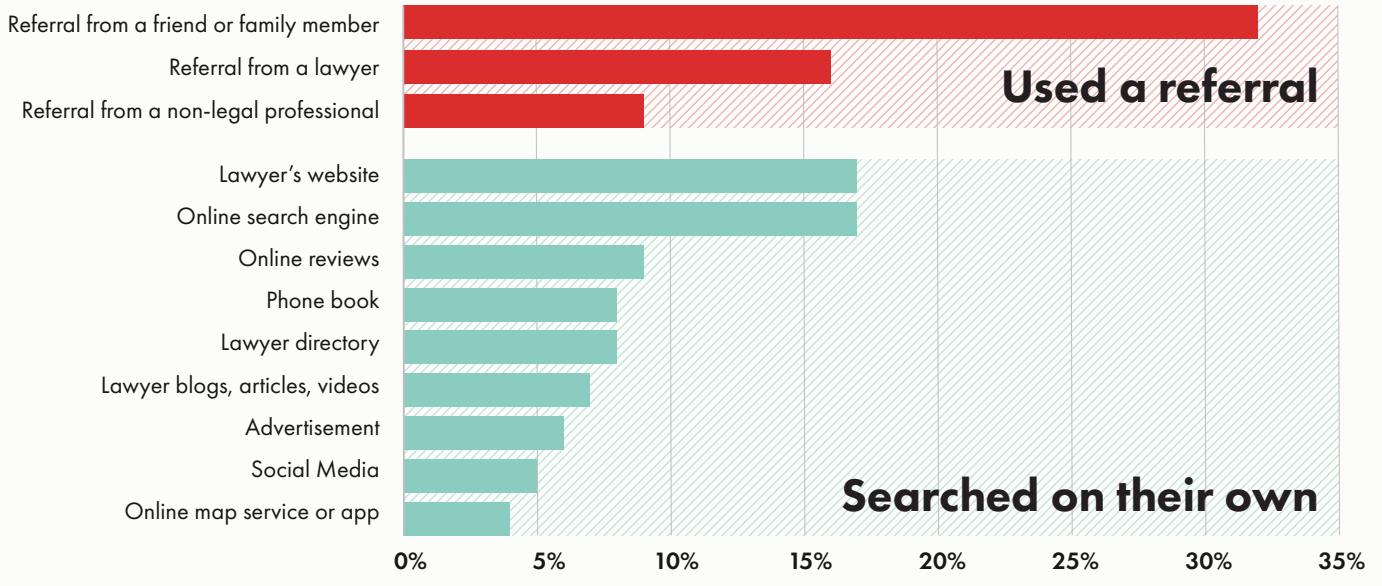
When we look at how clients shopped for a lawyer, we see that **59%** sought a referral of some kind. Friends and family members were the most common source for a referral (**32%**), followed by referrals from a lawyer (**16%**) or another non-legal professional (**9%**). (A non-legal professional could include an accountant, real estate agent, or someone else working in a profession related to a certain type of issue.)

Additionally, **18%** of clients said they would *never* seek a referral from a friend or family member, **17%** said they would *never* get a referral from a non-legal professional, and **14%** said they would *never* get a referral from another lawyer.

But referrals aren't the only way to find a lawyer—**57%** (about the same number that sought a referral) looked for a lawyer on their own. Methods such as using an online search engine (**17%**) and visiting a lawyer's website (**17%**) were the most common among those who have ever shopped for a lawyer.

These findings suggest that lawyers who focus on building their business from referrals only—while neglecting the many other sources out there—are missing out on significant business opportunities.

How clients searched



18% of clients said they would never seek a referral from a friend or family member

Referrals aren't the only way to find a lawyer

Is one method of searching for a lawyer better than the other? To answer this question, we identified which methods clients were most likely to use first—and then looked at whether those clients were likely to use other methods afterwards.

If clients find what they're looking for using one method, there would be no reason to use another method later on. Conversely, if clients can't find what they are looking for using one method, this would indicate that these methods aren't as useful to potential clients—and potentially less fruitful for law firms.

It turns out that clients are nearly just as likely to search for a lawyer through their own means first (**39%**) as they are to first seek a referral of any type (**45%**)—and **16%** indicated they couldn't remember. Online search engines were the most common first step for clients who didn't first seek a referral, but potential clients may use a range of resources as their first step to seeking a lawyer.

When we look at how mutually exclusive these two groups are to each other, the results show that there is relatively little overlap between those who seek a referral first and those who seek on their own through some other means:

- Of those who sought a referral first, only **16%** also looked on their own.
- Of those who looked on their own first, only **17%** also sought a referral.

While those who looked on their own were more likely to use more than one method, they didn't feel the need to also seek a referral. In other words, consumers tend to either seek referrals or do their own research to find a lawyer. Rarely do they do both.

Consumers tend to either seek referrals or do their own research to find a lawyer

Clients want information more than anything

In fact, **45%** of consumers who have experienced a legal issue agree that their challenge is finding a lawyer they are confident is right for them. Regardless of how they search for a lawyer, the majority of consumers indicated that each of the following were important to them:

- **77%** want to know a lawyer's experience and credentials (also ranked the most important).
- **72%** want to know what types of cases they handle.
- **70%** want a clear understanding of the legal process and what to expect.
- **66%** want an estimate of the total cost for their case.

While potential clients say they want an estimate of total cost for their case, that doesn't mean they don't see the value in hiring a good lawyer. **62%** who have ever hired a lawyer say it's worth paying a high price for a lawyer if they are very good.

Millennials are shifting attention online

When we look at the differences between younger generations compared to older ones, we can also see that perceptions and behaviors shift with younger generations.

For example, younger generations and those who have never hired a lawyer before find the whole experience of searching for a lawyer more challenging and intimidating. **39%** of Gen Z and **40%** of Millennials admit to being intimidated by lawyers compared to **30%** of Gen X and only **20%** of Boomers.

- Younger generations are more likely to care about a lawyer's website (**49%** of Gen Z and **48%** of Millennials compared to **34%** of Gen X and **21%** of Boomers).
- Younger generations are more likely to care about a firm's brand and image (**45%** of Gen Z and **36%** of Millennials compared to **28%** of Gen X and **19%** of Boomers).
- Younger generations are more likely to care about a firm's online reviews (**46%** of Gen Z and **53%** of Millennials compared to **39%** of Gen X and **25%** of Boomers).
- Younger generations are less likely to value referrals from lawyers (**47%** of Gen Z and **46%** of Millennials compared to **56%** of Gen X and **60%** of Boomers).

The takeaway? Firms looking to attract younger clientele, who likely have more potential for repeat business and long-term referrals, should consider focusing on digital channels where brand and image are important.

What does this mean for lawyers?

When it comes to shopping for a lawyer, consumers follow many paths. Seeking a referral may be the most common means, but many rely instead on other methods that focus heavily on online search and a firm's web presence. Increasingly, we also see younger generations prioritize electronic methods over referrals.

In other words, firms that focus only on building their referral network to find new business will miss out on growing opportunities to find new clients across other channels. Firms that want to maximize their opportunity for new business should look at marketing their firm across as many channels as possible—especially through online search and with their website.

Regardless of how firms promote their services, lawyers must ensure they provide the right information to prospective clients by highlighting their range of experience, making it clear what types of cases they handle, and providing a clear understanding of what to expect from a case and how to proceed.

Technology is making it increasingly easier to research law firms online—and firms that adapt to how clients look for their lawyer today, and in the future, will have the fullest opportunity for growing their business. Those that don't adapt will miss out on expanding their opportunities for finding new clients.

The next step is to do everything right when these clients eventually reach out—helping ensure better success in actually getting hired.

Technology is making it increasingly easier to research law firms online

Part 3

More than half of clients shop around

Marketing to potential clients is only part of the work required to actually get hired, and regardless of how clients look for a lawyer, there's a good chance they'll reach out to more than one.

44% of clients believe that they need to shop around and talk to more than one lawyer to find one that's right for them, and **57%** of those who have ever shopped for a lawyer say they contacted more than one law firm.

Even though clients are likely to shop around, firms that focus on client experience will have a better chance at making a great first impression—and deter them from looking any further. **42%** of consumers surveyed say that if they like the first lawyer they speak with they won't need to speak with any others.

An initial conversation with a law firm marks the beginning of that client's journey with the firm—and clients view that first interaction as an indicator for the overall experience of working with the firm. Leaving a bad impression will only drive potential clients away.

42% of consumers surveyed say that if they like the first lawyer they speak with they won't need to speak with any others

What do clients look for when first contacting a lawyer?

Making a good impression isn't just about picking up the phone or answering an email—clients need to have reason to believe that the lawyer they contact is the right lawyer for them.

Of those who have ever experienced a legal issue, **82%** agreed that timeliness was important to them. Clients also have an appetite for knowledge and want to get as much information about their case as possible:

- **81%** want a response to each question they ask.
- **80%** say it's important to have a clear understanding of how to proceed.
- **76%** also want to get a clear sense of how much their legal issue could cost.
- **74%** want to know what the full process will look like for their case.

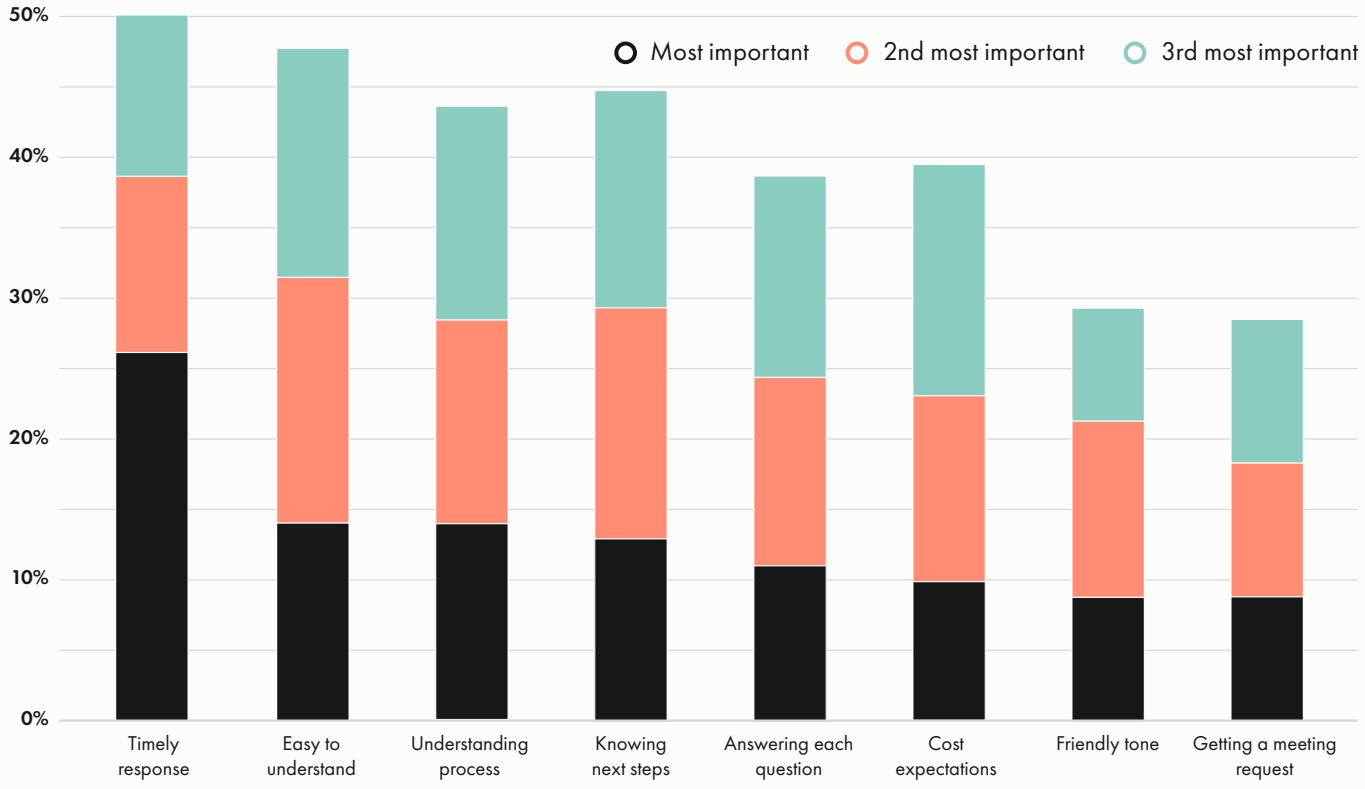
The friendliness and likeability of a lawyer's tone is also important to **64%**, but this isn't as common as the need to have a solid foundation for understanding their case and how to proceed.

When we asked consumers to rank what factors were most important to them when speaking with a law firm, responsiveness was ranked highest overall. But there was a relatively even distribution across each factor, suggesting that clients are conflicted on which is most important—and that they are in fact *all* important.

Lawyers need to give equal weight to how *quickly* they respond and how *well* they respond.

Importance to clients

Many factors rank high among clients



Law firms should respond within 24 hours

How quickly do potential clients expect firms to respond when leaving a phone message or email? **10%** expect a response within an hour, **24%** within a few hours, and **45%** within 24 hours. In other words, responding beyond 24 hours means missing the expectations of **79%** of those who reach out. Only **5%** of clients said they would expect a response beyond 72 hours.

Given that clients are likely to reach out to more than one firm when experiencing a legal problem, being the first to respond will help make a better impression.

Expected response times

79%

of consumers expect a response within

24hrs

% of clients expecting a response

% of expectations met when firms respond

Phone is the most important channel, but email and in-person are significant

Of those who indicated how they first reached out to a law firm, **68%** said they reached out by phone, **25%** by email or an electronic form, and **26%** in person.

Clients have diverse preferences for how they reach out to a lawyer. Firms that want to make the most of every potential opportunity for business should be prepared to deliver a great client experience from the start of every interaction, across a variety of methods.

Lawyers actually drive clients away

We asked clients what reasons they had for not hiring the lawyers they reached out to. **64%** indicated they contacted a law firm that never responded—either through phone or email. For any firm looking to find new business, not responding to potential clients means not getting hired.

But clients also agreed that there were many other reasons for not hiring some of the law firms they corresponded with, and these align with our findings in Section 2 of this report. Clients need information that confirms a firm can help them with their particular problem, and they need to know that the firm is ready to help.

- **65%** didn't get any indication on what to do next.
- **64%** didn't get a sense of how much their case would cost.
- **62%** didn't understand the process for their case.
- **61%** didn't get enough information they could understand.
- **52%** said the lawyer they spoke with wasn't likeable or friendly enough.

64% contacted a law firm that never responded

What does this mean for lawyers?

Most lawyers want more clients, yet many law firms are failing to convert the clients that reach out to them —specifically through phone or email. According to the consumers we surveyed, the law firms that aren't getting hired are the ones that do a poor job of responding to client inquiries or that don't provide the type of information that clients are looking for.

The consumer data in this section is illustrative of how firms can align their business strategies to focus on the client-experience axis of the Law Firm Maturity Model. Firms that want to increase how much they get hired should look at those first client interactions, as each one is a valuable sales opportunity for earning new business. Given that many clients shop around and speak to multiple law firms, firms that prioritize responsiveness with potential clients are likely to make a good impression. Firms that can demonstrate both responsiveness and provide quality experiences are the ones that will get hired.

To better understand just how well law firms respond to clients, and how they can improve, we put together an in-depth market analysis, which is explained in detail in the next section.

Firms that provide responsive, quality service will get hired more

Part 4

Putting 1,000 law firms to the test

It's not easy shopping for a lawyer in 2019. Our survey research shows that **32%** of clients who have ever shopped for a lawyer don't expect a law firm to get back to them, and **64%** of those who contacted a lawyer they didn't hire said a law firm didn't respond to their phone or email. Yet, **89%** of legal professionals we surveyed said that they respond to phone and email inquiries within 24 hours.

To assess how well law firms are prepared to meet the needs of potential clients today, we put them to the test. **We emailed 1,000 law firms and phoned 500 randomly selected from the same group.**

Designed to evaluate the responsiveness and quality of service provided by each firm, we hired a third-party research company to contact each firm with a brief list of questions that a typical potential client would have when they first reach out. The questions pertained to a particular legal issue tailored to the firm's practice areas and inquired about overall cost and options for booking a consultation.

The data from this analysis represents the first and only primary assessment of law firms of this magnitude, and the results provide strong implications for the state of client services—and indicate there is plenty of opportunity for firms to distinguish themselves from competitors.

We emailed 1,000 law firms and phoned 500 randomly selected from the same group

Building our sample

Our analysis assessed the client services provided by 1,000 randomly selected law firms in the United States. We tailored our outreach to correspond with the type of law practiced by each firm, across five different issue types:

- **Family** (child custody)
- **Criminal** (domestic abuse charge)
- **Bankruptcy** (debt elimination)
- **Employment** (racial discrimination)
- **Business** (incorporation)

To be eligible for our analysis, firms needed to have:

- An active web presence (such as a live website, a social page with activity in the three months prior to the study, or an active directory page).
- A publicly available email and phone number.
- Information available that indicated they handle legal issues related to the ones used in our study.

We also confirmed that all 1,000 law firms in our analysis received our email communications. For any emails that resulted in an email bounceback, we removed the associated law firm from our sample and replaced it with another to ensure that we achieved 1,000 successful email deliveries.

Law firms struggle with email

The results from our study show that the majority of law firms are unable to follow up with clients who reach out via email. **60%** of law firms didn't respond to our emails at all.

Given that this is the preferred method of initial outreach for **25%** of potential clients, this means that these firms are missing out on a sizable portion of their potential market.

The 24-hour window

Of those who did respond, **82%** did so within 24 hours. **11%** responded after 24 hours, and **7%** after 72 hours. There are a couple of takeaways from this. First, if a law firm is going to respond to a client inquiry, they'll likely respond in a day. Second, if a firm doesn't get back to their client inquiry in a day, there's a good chance they won't respond at all.

60% of law firms didn't respond to our emails

Getting information through email is hard

Few firms seem able to provide more than a brief response when communicating via email. Only **29%** of law firms that responded via email were able to provide a response that was timely, clear, answered at least one question, and provided some information on either booking a consultation or cost.

- **58%** had a likeable tone.
- **57%** provided information that was clear and easy to understand.
- **28%** provided clear next steps.
- **27%** referenced similar legal situations or demonstrated knowledge of the issue.
- **27%** provided some information on rates or overall cost.
- **13%** provided information on what to expect from the legal process.

While most email responses were still timely and within 24 hours, **71%** were unsatisfactory in terms of the information provided.

Only 28% of firms provided clear next steps

Lawyers prefer the phone

Even the firms that responded to us wanted to avoid email:

- **53%** of all the emails we received requested that we phone the office instead of communicating through email.
- **15%** of emails didn't provide any information and asked only that we phone them instead.

Law firm email scorecard

% Firms	Evaluation	Criteria
0.5% (2 law firms)	Excellent	• Responded within 24 hours • Professional and courteous • Clear and easy to understand • All questions answered regarding the matter and the lawyer's ability to help • Detailed information on what to expect from the process and next steps • Detailed information on consultations and overall rates or cost
5% (20 law firms)	Good	• Responded within 24 hours • Not confusing • At least half the questions answered regarding the matter and the lawyer's ability to help • Some information on what to expect from the process and next steps • Some information on consultations and overall rates or cost
23% (93 firms)	Adequate	• Responded within 24 hours • Not confusing • At least one question answered regarding either the matter or the lawyer's ability to help • Minimal information on either consultations or overall rates or cost
71% (284 firms)	Unsatisfactory	• Did not meet the criteria for an adequate response

Law firms are better at answering their phones but rarely return calls

Compared to email, law firms were more responsive through phone, but not by much:

- **56%** of law firms answered our calls.
- **39%** of our calls went to voicemail—of which **57%** didn't return our call within 72 hours.
- **5%** of our calls were unanswered.

In total, **73%** of firms either picked up or phoned us back—meaning that, **we were unable to reach 27% of law firms by phone**.

57% of law firms never phoned us back

Law firms don't provide enough information over the phone

While many firms picked up the phone to speak with us, few were able to provide a lot of key information, and even fewer were able to demonstrate their knowledge and experience in working with similar types of cases. Many firms would only discuss information related to a case or questions related to rates and cost in a follow-up meeting.

- **56%** provided rate information (hourly or fixed fees)—**9%** provided a total cost estimate.
- **50%** explained the legal process and indicated next steps.
- **49%** answered most questions asked. **11%** would only answer questions in a follow-up appointment.
- **43%** would not discuss rates or cost over the phone.
- **11%** referenced case examples with contextual information.

43% of firms wouldn't discuss rates or cost over the phone

Law firm phone scorecard

We calculated an overall conversation score that takes into account how well each firm we spoke with handled our communications. This score was calculated by averaging performance scores for:

- Number of questions answered
- Demonstrated experience with the particular case
- Information on rates or overall cost
- Information on next steps

% Firms	Evaluation	Criteria
7% (20 law firms)	Excellent	These firms were able to provide detailed information on nearly all content criteria (scoring 80% to 100%)
9% (26 law firms)	Good	These firms did not meet all requirements but provided detailed information for approximately 75% of our criteria (scoring 70% to 80%)
22% (62 law firms)	Adequate	These firms provided the minimum amount of information to be deemed adequate (scoring 50% to 70%)
61% (171 law firms)	Unsatisfactory	These firms did not meet the criteria for more than half of our performance drivers (scoring less than 50%)

Lawyers provide more information than assistants

Lawyers generally provided more information when they answered the phone compared to assistants.

- **66%** of lawyers who we spoke to over the phone were able to answer the majority of questions we asked them compared to **43%** of assistants.
- **38%** of lawyers provided detailed information about the firm's experience handling similar types of cases compared to **13%** of assistants.
- **66%** of lawyers provided rate information (either hourly or fixed fee) compared to **54%** of assistants.

Lawyers picked up the phone **24%** of the time compared to **71%** of calls that were answered by an assistant (**5%** were answered by an automated phone system). While lawyers are likely much better equipped to provide this type of information over the phone to a potential client, there were still a large number of calls answered by an assistant that were able to provide this information—either by the assistant or by transferring directly to someone else.

While many lawyers have room to improve their initial communications, equipping assistants with the ability to better answer questions and provide information is a major opportunity for the legal industry to improve client services. Making lawyers more available to potential clients will also help get them the information they need quicker.

Little gets communicated through voicemail

Only **43%** of law firms responded to our voicemails. For our analysis, all returned calls were forwarded to a voicemail system of our own, of which **86%** of responding firms left messages (**14%** ended their call without leaving a message). Similar to email, most of these responses (**86%**) came within 24 hours, indicating that firms are either likely to get back to their clients within a day or not at all.

When leaving a voicemail, few firms provided information in response to the questions we asked.

- **36%** provided rate information (hourly or fixed fees)—**0%** provided a total estimated cost.
- **14%** explained the legal process and provided next steps.
- **4%** answered most of our questions.
- **0%** referenced cases with contextual case information.

We calculated voicemail scores based on the same criteria as our phone conversation scorecard. From the data we collected, it's clear that being able to answer when a client calls gives the firm a much better opportunity to provide information and service. Missing the call and having to deal with voicemail is unproductive for everyone.

Law firm voicemail scorecard

% Firms	Evaluation	Criteria
0% (0 law firms)	Excellent	These firms were able to provide detailed information on nearly all content criteria (scoring 80% to 100%)
0% (0 law firms)	Good	These firms did not meet all requirements but provided detailed information for approximately 75% of our criteria (scoring 70% to 80%)
4% (3 law firms)	Adequate	These firms provided the minimum amount of information to be deemed adequate (scoring 50% to 70%)
96% (81 law firms)	Unsatisfactory	These firms did not meet the criteria for more than half of our performance drivers (scoring less than 50%)

Comparisons between email and phone

Not surprisingly, firms that responded to our emails were more likely to provide better phone service —but not by much.

Of those who answered our emails:

- **60%** picked up the phone, compared to **54%** for those who didn't answer our email.
- **36%** went to voicemail, compared to **41%** of those who didn't answer our email.
- **58%** answered our voicemail, compared to **34%** of those who didn't answer our email.
- **3%** didn't get answered by a person or voicemail, compared to **5%** of those who didn't answer our email.

Those who didn't respond to our emails were slightly more likely to have a poor conversation score (**73%**) than those who did respond to their email (**63%**).

What does this mean for lawyers?

Based on our surveys, client expectations for law firms are low—and data from our email and phone analysis suggests this is rightly so. When it comes to bringing in new clients, firms that exceed these fairly reasonable expectations are the ones more likely to get hired.

In the context of the Law Firm Maturity Model, this assessment suggests that the majority of firms have a long way to go in progressing along the client experience axis to becoming a responsive firm. Firms that are too busy to respond or to take the time to deliver quality communications may also be suffering from a lack of efficient processes that allow for this type of focus.

Regardless of the reason for not providing better client experiences—whether it's that firms aren't willing or aren't able to focus more on this aspect of their firm—these types of service experiences will undoubtedly hold back firms from achieving high-growth success.

At the same time, this deficiency presents a major opportunity for law firms to innovate and differentiate themselves within their markets. Firms that meet—or exceed—expectations will capture more clients as they reach out. Firms that are able to then fulfill their client work in a similar manner will also grow their referral opportunities down the road.

71% of firms didn't meet the criteria for an adequate email response

Part 5

How prepared is today's lawyer to drive their firm's success?

When it comes to ensuring their firm's success, how prepared are today's legal professionals? To learn more about how lawyers think about success—and where they struggle—we surveyed over 2,500 legal professionals to learn more about how they think about and plan their success.

It turns out the vast majority of law firms are focused on growth.

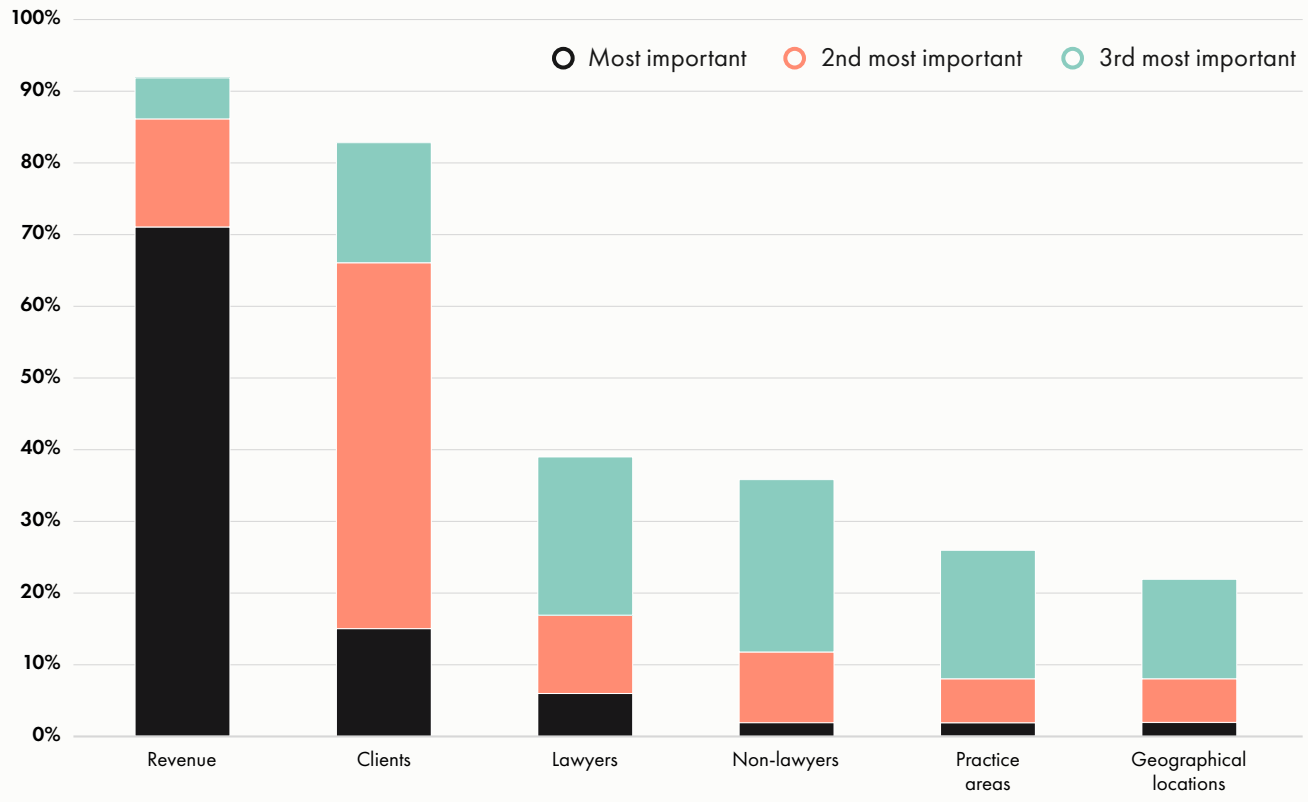
87% of lawyers agree they want their firms to grow over the next three years—and **67%** say they want to grow more than a little. And when it comes to growth, lawyers rank revenues and client base as the **top two** areas they want to see grow. But how prepared are lawyers to achieve these goals?

There is no question: being a lawyer is a tough occupation. **76%** of lawyers say they are overworked and **68%** say they are underappreciated. On the bright side, the majority love being a lawyer (**69%**) and really like working with clients (**82%**).

But, as the Law Firm Maturity Model illustrates, there are two critical components—beyond having expert knowledge of the law and giving great legal advice—to running a successful business in legal. One component is the effort that goes into understanding and delivering quality client experiences. The other is organizing everything in the firm to be productive and making sure everything gets done in an efficient manner. Both are essential to achieving the type of growth law firms strive for.

87% of lawyers want their firms to grow

Factors representive of firm growth



Half of managing lawyers aren't confident in managing their business

When it comes to those responsible for managing the business aspects of a firm, our research shows that a significant proportion of managing lawyers don't feel prepared to handle the business side of a law firm. **While 92% are very confident in their skills as a lawyer, only 53% are confident in running the business side of their firm.**

Despite being a critical component to the growth and overall health of a firm, lawyers are rarely trained in the management side of running a practice as part of their education or licensing. In fact, only **7%** agree that law school prepared them to run the business side of their firm. Bar associations are a slightly better resource, but not by much: only **23%** agree that their bar association provides adequate business training.

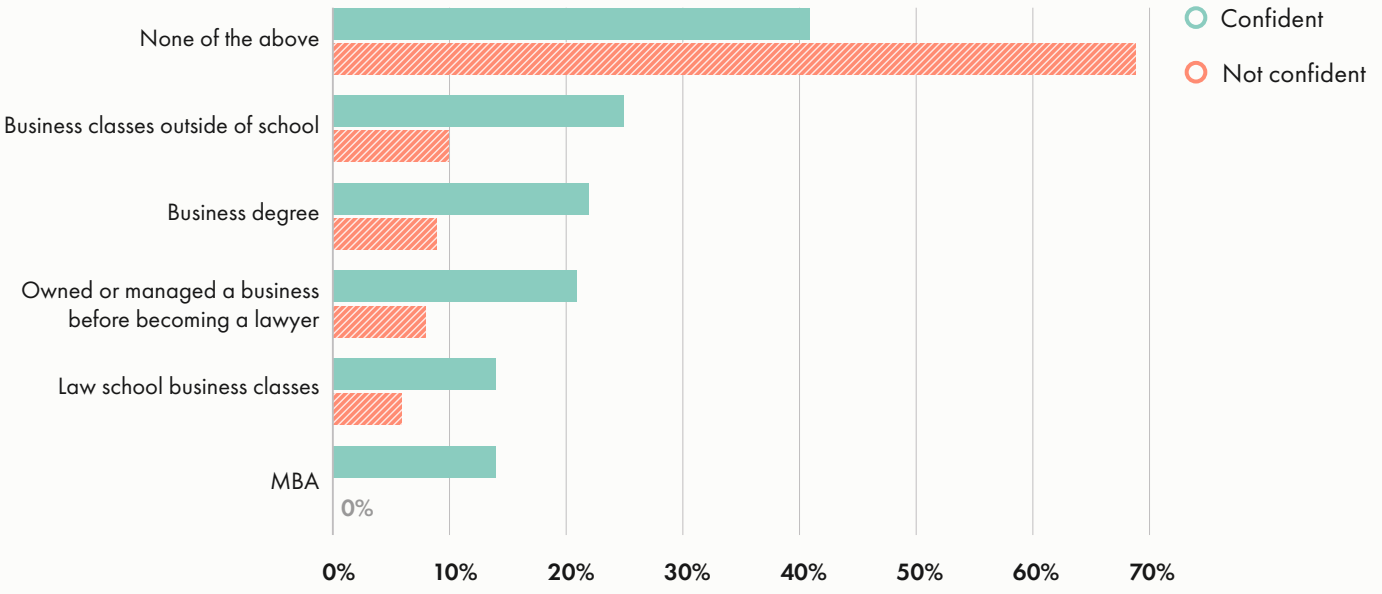
Only 53% of managing lawyers are confident in running their business

Training and experience brings confidence

To better understand what makes some lawyers more confident than others, we looked at the range of training and experience between each group.

As it turns out, those who are confident are much more likely to have some prior business training or experience —which may include having an MBA (**14%**), owning or running a business prior to becoming a lawyer (**21%**), majoring in business in college (**22%**), taking business classes outside a formal school setting (**25%**), or taking business-management classes in law school. **41%** say they have no prior training or experience.

Education and experience



Of those who aren't confident in running the business side of their firm, **69%** report having no business training at all. Additionally, **72%** say they don't know enough about running a business.

Those confident in running the business side of their practice are also much more prepared and more likely to invest time and resources into their learning. **62%** of those confident in managing the business side of their firm frequently read books or articles related to running or growing a business and **36%** frequently take courses. Only **43%** of those not confident spend time reading about running their business better, and only **18%** take courses.

What differentiates those who know how to run a business?

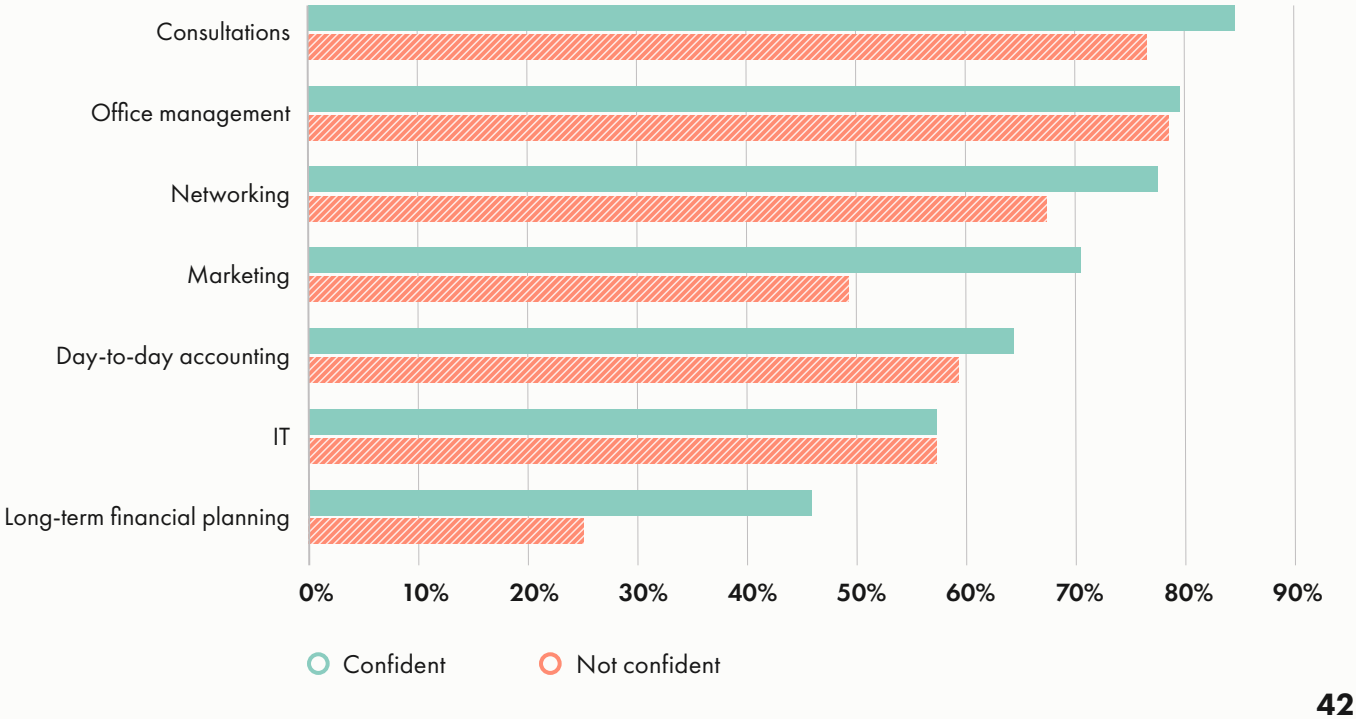
Lawyers who are confident about managing the business side of their firm tend to worry a lot less about it. Only **32%** are worried about something falling through the cracks compared to **78%** who aren't confident about their business.

To get a better sense of how lawyers prioritize their work in managing their firm, we asked lawyers how often they perform various tasks or duties and compared responses between those confident in running their firms to those who aren't.

The responses show that those confident in running their firm are more engaged in some key business aspects of their firm than lawyers who aren't confident in managing the business aspects of their firm.

Two areas in particular show a significant disparity in how those who are confident spend their time compared to those who are not confident. For one, even though both cohorts indicated they spend generally less time on long-term financial planning, only **25%** of those not confident did at least sometimes, compared to **46%** of those confident in running their business. The other area to call out is marketing, which more confident lawyers (**70%**) indicated spending time on compared to those not confident (**49%**).

Business areas firm managers often engage in



What does this mean for lawyers?

A famous study showed that **93%** of Americans believe they are above average when it comes to driving ability (an obvious statistical impossibility, since only **50%** can be above average). The study is illustrative of a cognitive bias known as illusory superiority, which sees individuals overestimate their own abilities in relation to others.

Those confident in running their firm are more engaged in the business

What's interesting is that when it comes to the practice of law, lawyers don't have this same overconfidence. While **73%** of lawyers agree that they're different than most lawyers, only **56%** agree that they are better than most lawyers. In an industry where success is often dictated by the facts of a case and the judicial system outside of any one lawyer's control, it's often most practical to focus on what a lawyer *can* control: achieving the best possible outcome for a matter.

The same goes for running a successful business. While **87%** of lawyers want to see their firm grow over the next three years, not every lawyer knows how. Focusing on success and increasing revenues on their own are outcomes that may be at least partially outside of the firm's control. Instead, focusing on key inputs discussed in this report provide important leverage points that are both controllable and impactful. The client experience and firm performance axes within the Law Firm Maturity Model provide two critical vectors to prioritize.

As discussed in the first section of this report, some firms know how to achieve year-over-year growth, while others see their prospects dwindle. Knowing how to earn clients and maintain high standards for business are two key factors to success.

Sections 2 and 3 in this report outline a comprehensive look at how clients shop for a lawyer and what they look for when they reach out. Ultimately they're looking for clear information and responsiveness. As Section 4 shows, these are qualities that many firms lack.

Managing a business effectively means getting the most opportunity out of the resources available. Those who have training or experience in running a business are much more prepared to spend time learning about and applying themselves to the business side of their firm—for the betterment of both the firm and their clients.

Confidence alone may not be enough to grow a firm's business, but there's a good chance that future analysis will show that improving the business side of a law firm—not just the ability to practice law—leads to greater firm success in the long term.

Key business inputs are both controllable and impactful

Part 6

Hourly rates and KPI data

For the past four years, the *Legal Trends Report* has provided benchmarking data on some of the most critical business metrics that determine law firm performance. In this section, we've updated the data for 2019 and included new discussions on why this data is relevant to firms today.

Hourly rate and the Billable Hour Index: How much does a lawyer typically charge per hour?

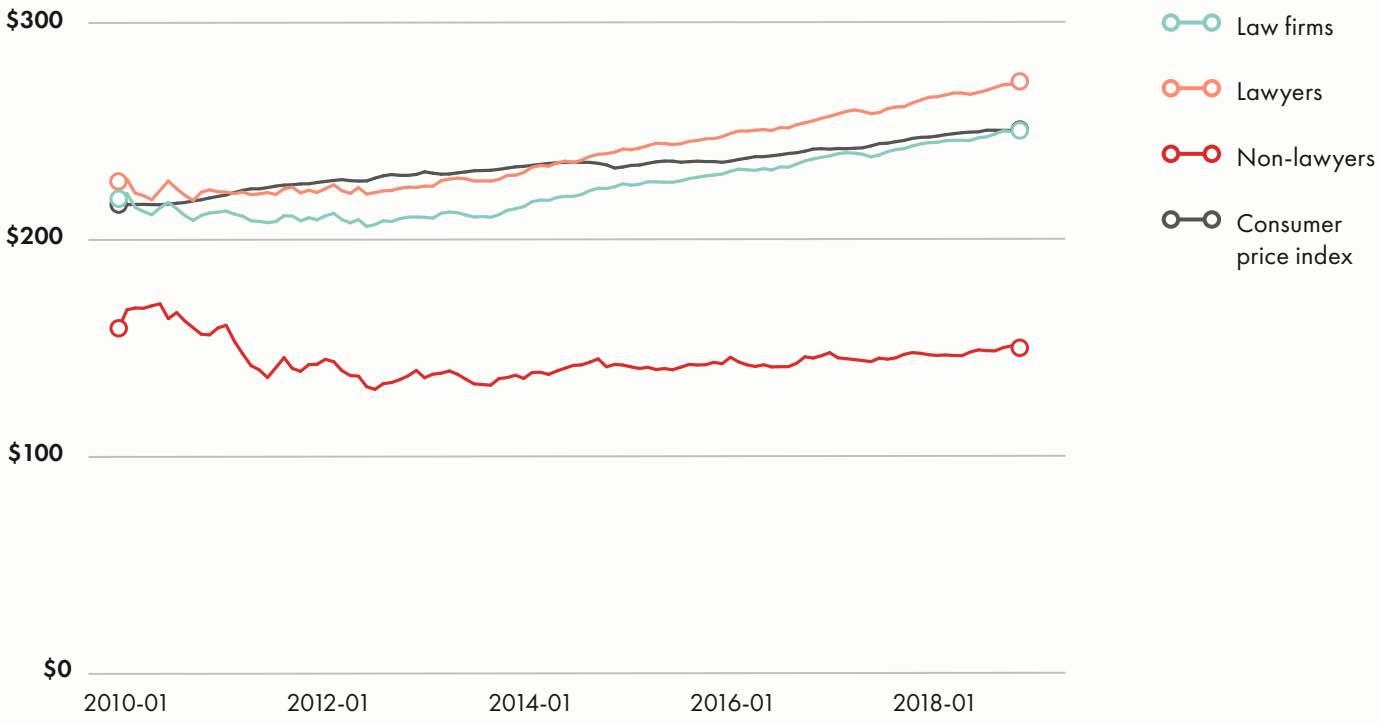
As a service-based profession, any revenue earned by a law firm almost exclusively comes from the time a lawyer puts toward billable work on behalf of their clients—and hourly billing is still the predominant method for billing among law firms. As such, we analyze hourly billing rates to determine how revenue-earning potential changes over time.

In what we call the Billable Hour Index, we see that after remaining relatively flat up until 2014, hourly rates have steadily increased on average to $253 in 2019.

This trend follows closely with the Consumer Price Index, which we use as a benchmark indicator corresponding to the actual purchasing power and living wages in the United States.

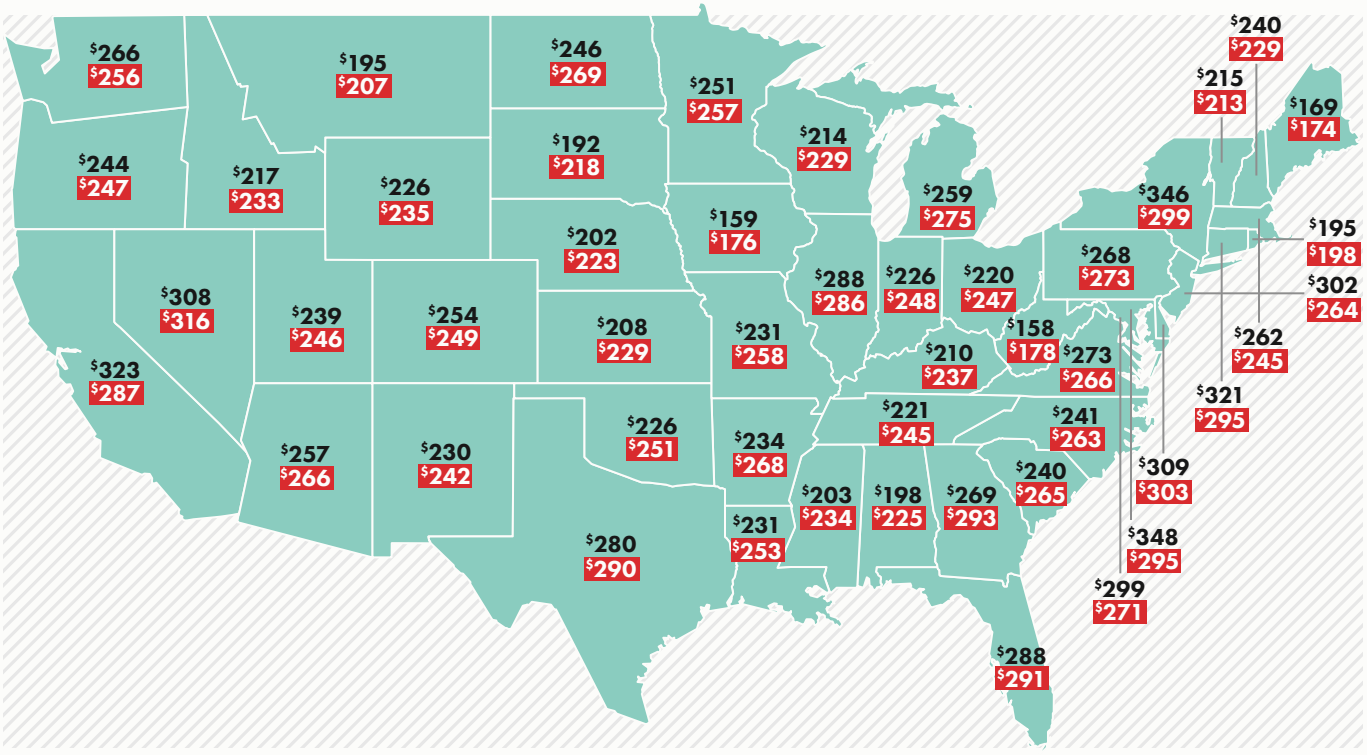
Similar to previous years, non-lawyer rates have remained relatively stagnant.

Billable Hour Index



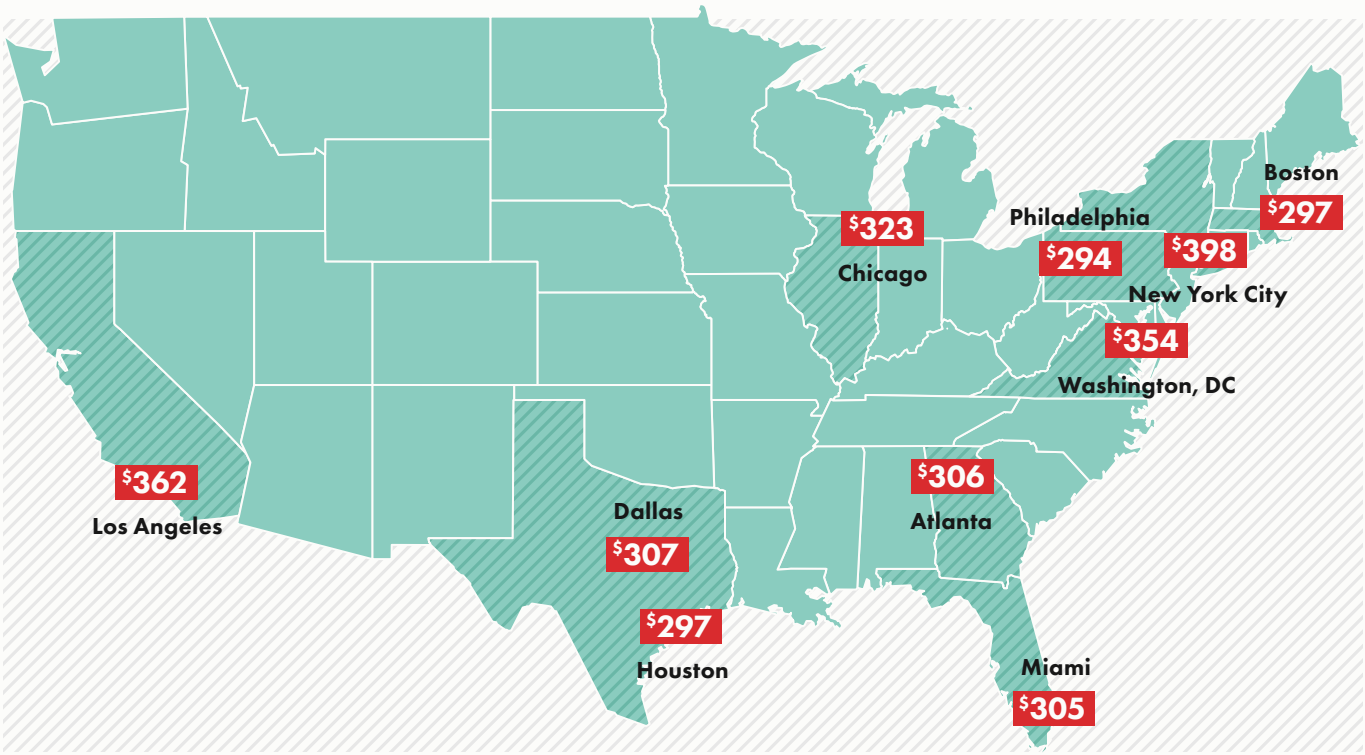
Regional rates adjusted for cost of living

Similar to how we compare lawyer rates to the Consumer Price Index, we also compare average regional rates to estimations on the overall cost of living within each state. "Actual" rates are the rates that a lawyer charges, and "adjusted" rates have been adjusted to reflect cost of living data—providing a better point of comparison in terms of how much a lawyer earns relative to their purchasing power within each state.



Actual rate Adjusted rate

Hourly rates for large metropolitan areas



Key business metrics for firm performance

Since 2016, we've defined specific business metrics to reflect how efficient law firms are at performing billable tasks in relation to invoicing and collecting payment. Utilization, realization, and collection rates provide powerful insights into how productive a firm is in generating revenue.

Utilization rate: How much of a day is dedicated to earning money for the firm?

Utilization rate measures the average time a lawyer puts toward billable work on a given day. When compared to the total number of hours available in a day, we get a percentage that we call a utilization rate.

Based on aggregated and anonymized data from tens of thousands of lawyers, we determined that the average lawyer worked just **2.5 hours** of billable work each day in 2018. When we compare this to a standard 8-hour workday, we calculate a national average of **31%** utilization for the typical lawyer.

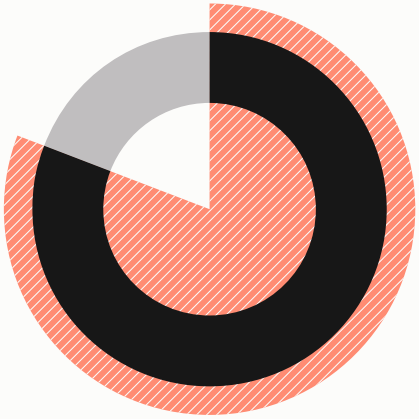
Average utilization rates for the legal industry have stayed consistent in the four years we've been publishing the *Legal Trends Report*. While this number is much lower than what other industry reports publish, other reports are based on self-reported survey data, which can often suffer from social desirability biases when it comes to reporting sensitive information like earnings. People are also more likely to report on the good times or fail to take into account the ups and downs of a broader time scale for a full working year.

The benefit of this analysis is that it looks objectively at data trends across tens of thousands of legal professionals over the course of a full year.

Utilization rate

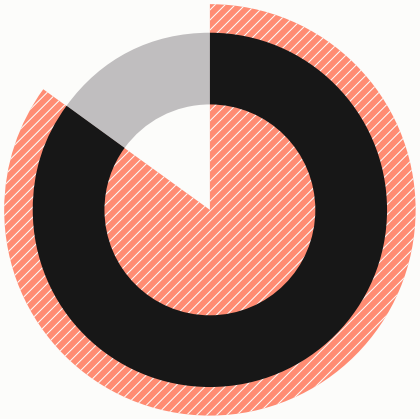
Number of billable hours worked ÷ number of hours in a day = **31%**

Realization rate



Number of billable hours invoiced ÷ number of hours worked = **81%**

Collection rate



Number of hours collected ÷ number of hours invoiced = **86%**

The average lawyer worked just 2.5 hours of billable work each day in 2018

Realization rate: How much billable work makes it to an invoice?

Realization measures the amount that a firm invoices compared to the amount of billable work performed at a law firm.

We know that not every hour worked gets billed for. In fact, **19%** of the time lawyers work doesn't make it to a bill. There could be a number of reasons for this. Last year's report suggests the most common reasons for lawyers discounting billable work are: empathy for the client, the client's ability to pay, or the belief that too much time was tracked to begin with.[1]

[1]2018 *Legal Trends Report*, **page 61**.

Regardless of the reason behind the loss in realization, the data suggests that a significant amount of time is wasted on work that doesn't earn any revenue. Firms can improve realization by ensuring the work they take on will be billable in the first place, or making sure they have the processes in place to ensure that work makes it to a bill.

Collection rate: How much billed time gets collected?

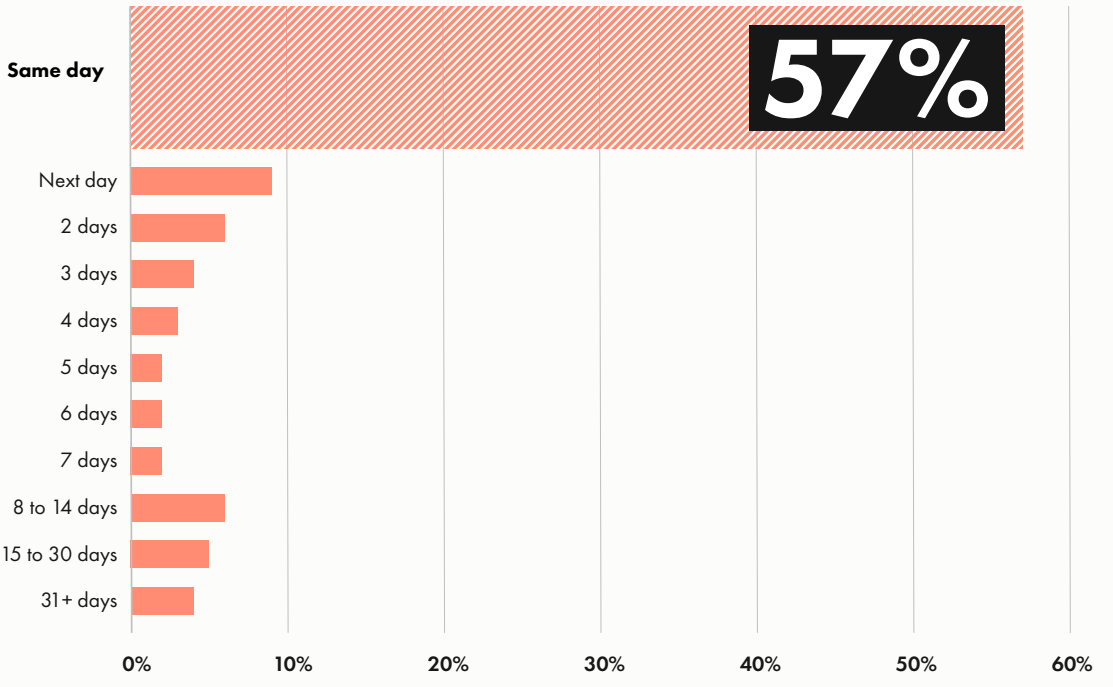
Collection measures the amount that a firm collects compared to the amount invoiced at a law firm.

Not every hour billed gets collected upon. Of all hours invoiced to clients, **14%** never get paid. This could mean that clients just aren't able to afford their legal bills, or it could mean that law firms don't do a good job of following up on their invoices. Regardless of the underlying cause, low collection rates mean money earned gets left on the table, leading to firms suffering costly revenue shortfalls.

One way to make fee payments easier for both clients and firms is to use electronic payments. According to survey data from last year's *Legal Trends Report*, **50%** of clients are more likely to hire a lawyer who takes electronic payments, **47%** are more likely to hire a lawyer who accepts automated payments or fund transfers, and **40%** would never hire a lawyer who didn't take credit or debit cards.

Electronic payments also get paid faster, making collections easier and saving follow-ups when bills are past due. In fact, **57%** of electronic payments get paid within the same day they are billed, and **85%** get paid within a week.

How quickly electronic payments get paid after billing



Data provided by LawPay

LawPay
Powering Clio Payments

57% of electronic payments get paid within the same day

The lawyer's funnel

When put together, these utilization, realization, and collection rates make up the lawyer's funnel to earning revenue for the firm. The largest potential for earning is at the top, and that potential shrinks at each stage—which means that each stage is a critical opportunity for improving firm earnings.

To illustrate the devastating effect that the funnel can have on law firm revenue, we can calculate an average effective rate based on industry averages.

Based on an average industry rate of $253, a lawyer can expect to bring in $2,024 of revenue for the firm if they billed for a full 8-hour day.

Since the average lawyer only puts 31% of an 8-hour day toward billable work, this reduces maximum potential daily earnings to $627.

When we apply an 81% realization rate, average daily earnings shrink to $508.

Finally, when factoring in an 85% collection rate, average effective daily earnings fall to $432.

The lawyer's funnel

Earning potential shrinks at each stage of the funnel

Appendix A

Hourly rates and KPIs by state

Hourly rates by state

State	Law firms	Lawyers	Non-lawyers	State	Law firms	Lawyers	Non-lawyers
AL	$188	$198	$110	**NC**	$217	$241	$122
AR	$219	$234	$121	**ND**	$228	$246	$160
AZ	$228	$257	$135	**NE**	$195	$202	$182
CA	$295	$323	$172	**NH**	$224	$240	$126
CO	$229	$254	$133	**NJ**	$288	$302	$218
CT	$304	$321	$202	**NM**	$212	$230	$122
DC	$321	$348	$169	**NV**	$275	$308	$166
DE	$272	$309	$170	**NY**	$327	$346	$204
FL	$259	$288	$146	**OH**	$208	$220	$127
GA	$251	$269	$152	**OK**	$207	$226	$107
IA	$155	$159	$126	**OR**	$222	$244	$122
ID	$206	$217	$118	**PA**	$258	$268	$183
IL	$270	$288	$158	**RI**	$173	$195	$89
IN	$212	$226	$125	**SC**	$208	$240	$107
KS	$201	$208	$132	**SD**	$189	$192	$105
KY	$199	$210	$112	**TN**	$206	$221	$110
LA	$216	$231	$95	**TX**	$247	$280	$137
MA	$254	$262	$169	**UT**	$216	$239	$123
MD	$276	$299	$172	**VA**	$255	$273	$166
ME	$159	$169	$108	**VT**	$205	$215	$89
MI	$241	$259	$134	**WA**	$238	$266	$135
MN	$233	$251	$139	**WI**	$205	$214	$151
MO	$208	$231	$120	**WV**	$154	$158	$111
MS	$185	$203	$115	**WY**	$215	$226	$142
MT	$183	$195	$103				

Adjusted rates by state

State	Law firms	Lawyers	Non-lawyers	State	Law firms	Lawyers	Non-lawyers
AL	$214	$225	$126	**NC**	$237	$263	$133
AR	$250	$268	$138	**ND**	$249	$269	$175
AZ	$237	$266	$140	**NE**	$215	$223	$201
CA	$263	$287	$153	**NH**	$213	$229	$120
CO	$225	$249	$130	**NJ**	$252	$264	$191
CT	$280	$295	$185	**NM**	$223	$242	$129
DC	$272	$295	$143	**NV**	$282	$316	$170
DE	$267	$303	$166	**NY**	$282	$299	$177
FL	$261	$291	$147	**OH**	$232	$247	$142
GA	$272	$293	$165	**OK**	$230	$251	$119
IA	$172	$176	$139	**OR**	$224	$247	$123
ID	$220	$233	$127	**PA**	$263	$273	$186
IL	$268	$286	$157	**RI**	$176	$198	$90
IN	$232	$248	$136	**SC**	$230	$265	$118
KS	$222	$229	$145	**SD**	$215	$218	$120
KY	$224	$237	$126	**TN**	$229	$245	$121
LA	$236	$253	$104	**TX**	$256	$290	$142
MA	$237	$245	$158	**UT**	$223	$246	$126
MD	$250	$271	$156	**VA**	$248	$266	$162
ME	$163	$174	$112	**VT**	$202	$213	$88
MI	$256	$275	$142	**WA**	$230	$256	$130
MN	$239	$257	$142	**WI**	$220	$229	$162
MO	$232	$258	$134	**WV**	$173	$178	$125
MS	$213	$234	$132	**WY**	$223	$235	$147
MT	$194	$207	$110				

Hourly rates by practice area

Practice area	Law firms	Lawyers	Non-lawyers	Practice area	Law firms	Lawyers	Non-lawyers
Administrative	$206	$260	$112	**Government**	$168	$170	$99
Appellate	$272	$283	$120	**Immigration**	$271	$299	$201
Bankruptcy	$307	$340	$158	**Insurance**	$209	$226	$100
Business	$281	$295	$151	**Intellectual Property**	$326	$340	$190
Civil Litigation	$258	$276	$136	**Juvenile**	$86	$87	$74
Civil Rights/ Constitutional Law	$298	$332	$135	**Mediation/ Arbitration**	$286	$313	$88
Collections	$212	$239	$132	**Medical Malpractice**	$192	$225	$109
Commercial/ Sale of Goods	$289	$299	$135	**Personal Injury**	$200	$236	$115
Construction	$238	$260	$118	**Real Estate**	$273	$286	$186
Contracts	$251	$259	$151	**Small Claims**	$194	$200	$160
Corporate	$304	$318	$158	**Tax**	$301	$325	$176
Criminal	$161	$163	$134	**Traffic Offenses**	$255	$275	$179
Elder Law	$225	$246	$145	**Trusts**	$281	$319	$158
Employment/ Labor	$296	$311	$164	**Wills & Estates**	$255	$289	$150
Family	$234	$261	$139	**Worker's Compensation**	$162	$155	$193

Utilization by state

State	Lawyers	Non-lawyers	State	Lawyers	Non-lawyers
AL	34%	19%	**NC**	28%	19%
AR	27%	15%	**ND**	35%	17%
AZ	29%	23%	**NE**	36%	34%
CA	32%	25%	**NH**	25%	13%
CO	33%	25%	**NJ**	32%	24%
CT	28%	16%	**NM**	33%	15%
DC	30%	27%	**NV**	34%	25%
DE	35%	22%	**NY**	29%	22%
FL	30%	22%	**OH**	33%	22%
GA	27%	18%	**OK**	32%	17%
IA	38%	21%	**OR**	30%	18%
ID	34%	15%	**PA**	31%	19%
IL	34%	21%	**RI**	33%	32%
IN	32%	17%	**SC**	32%	22%
KS	31%	10%	**SD**	32%	9%
KY	29%	16%	**TN**	27%	16%
LA	27%	17%	**TX**	30%	25%
MA	30%	20%	**UT**	36%	29%
MD	28%	21%	**VA**	29%	22%
ME	37%	19%	**VT**	28%	19%
MI	30%	19%	**WA**	34%	25%
MN	30%	17%	**WI**	36%	23%
MO	31%	22%	**WV**	34%	12%
MS	26%	16%	**WY**	28%	16%
MT	35%	18%			

Realization and collection by state

State	Realization Rate	Collection Rate	State	Realization Rate	Collection Rate
AL	78%	84%	**NC**	79%	84%
AR	80%	88%	**ND**	88%	91%
AZ	81%	84%	**NE**	72%	87%
CA	80%	86%	**NH**	85%	90%
CO	88%	89%	**NJ**	79%	82%
CT	85%	83%	**NM**	80%	90%
DC	66%	83%	**NV**	80%	85%
DE	72%	89%	**NY**	74%	80%
FL	74%	86%	**OH**	82%	87%
GA	80%	87%	**OK**	85%	85%
IA	81%	83%	**OR**	86%	89%
ID	89%	86%	**PA**	80%	86%
IL	83%	83%	**RI**	79%	91%
IN	73%	84%	**SC**	89%	88%
KS	76%	89%	**SD**	84%	89%
KY	86%	87%	**TN**	74%	85%
LA	74%	87%	**TX**	83%	87%
MA	83%	88%	**UT**	89%	83%
MD	79%	88%	**VA**	85%	87%
ME	87%	89%	**VT**	87%	90%
MI	82%	86%	**WA**	89%	88%
MN	86%	90%	**WI**	81%	88%
MO	81%	85%	**WV**	61%	83%
MS	75%	81%	**WY**	92%	87%
MT	91%	88%			

Realization and collection by practice area

Practice area	Realization rate	Collection Rate	Practice area	Realization rate	Collection Rate
Administrative	53%	86%	**Government**	95%	98%
Appellate	83%	84%	**Immigration**	73%	79%
Bankruptcy	71%	72%	**Insurance**	61%	86%
Business	90%	88%	**Intellectual Property**	86%	91%
Civil Litigation	82%	85%	**Juvenile**	80%	86%
Civil Rights/ Constitutional Law	14%	82%	**Mediation/ Arbitration**	88%	90%
Collections	87%	88%	**Medical Malpractice**	63%	87%
Commercial/ Sale of Goods	87%	88%	**Personal Injury**	44%	91%
Construction	95%	90%	**Real Estate**	87%	89%
Contracts	78%	90%	**Small Claims**	87%	83%
Corporate	89%	88%	**Tax**	86%	89%
Criminal	70%	83%	**Traffic Offenses**	71%	85%
Elder Law	75%	73%	**Trusts**	86%	92%
Employment/ Labor	70%	91%	**Wills & Estates**	79%	89%
Family	91%	83%	**Worker's Compensation**	75%	96%

Average case value by practice area

Practice area	P10	P50	P90	Mean
Administrative	$150	$774	$6,000	$2,982
Appellate	$428	$2,380	$21,038	$8,556
Bankruptcy	$400	$1,295	$3,590	$2,390
Business	$184	$709	$4,013	$2,063
Civil Litigation	$218	$1,284	$10,402	$5,021
Civil Rights/Constitutional Law	$285	$2,736	$31,923	$12,251
Collections	$150	$488	$2,843	$1,353
Commercial/Sale of Goods	$200	$990	$6,375	$3,181
Construction	$300	$1,500	$10,940	$5,552
Contracts	$158	$600	$3,000	$1,543
Corporate	$200	$860	$5,348	$2,882
Criminal	$165	$756	$3,500	$1,567
Elder Law	$199	$925	$7,000	$2,614
Employment/Labor	$220	$1,251	$9,345	$4,367
Family	$280	$1,675	$8,019	$3,575
Government	$152	$500	$3,211	$1,919
Immigration	$150	$900	$3,690	$1,510
Insurance	$316	$1,960	$9,900	$4,298
Intellectual Property	$200	$750	$3,000	$1,985
Juvenile	$170	$561	$2,422	$1,126
Mediation/Arbitration	$180	$676	$2,925	$1,493
Medical Malpractice	$405	$6,000	$18,887	$8,981
Personal Injury	$281	$1,901	$8,333	$3,728
Real Estate	$175	$582	$3,218	$1,520
Small Claims	$150	$500	$1,675	$817
Tax	$125	$490	$4,496	$1,924
Traffic Offenses	$122	$300	$2,000	$727
Trusts	$250	$1,400	$5,977	$2,867
Wills & Estates	$210	$800	$3,345	$1,592
Worker's Compensation	$432	$2,188	$9,214	$3,970

Appendix B

App data collection

App data collection

The *Legal Trends Report* uses aggregated and anonymized data collected from the Clio platform, which gives us the foundation to identify informative and interesting patterns to observe and investigate. By synthesizing actual usage data, we're able to identify trends that would be otherwise invisible to most firms.

The *Legal Trends Report* has been prepared using data aggregated and anonymized from the usage activity from tens of thousands of legal professionals. These customers were included in our data set using the following criteria:

- They were paid subscribers to Clio. Customers who were evaluating the product via a free trial or were using Clio as part of our Academic Access Program were not included.
- They were located in the contiguous United States. This includes the District of Columbia but excludes Hawaii and Alaska. No customers in other countries were included.
- Any data from customers who opted out of aggregate reporting were excluded.
- Outlier detection measures were implemented to systematically remove statistical anomalies.

Data usage and privacy

The security and privacy of customer data is our top priority at Clio. In preparing the *Legal Trends Report*, Clio's data operations team observed the highest standard of data collection and reporting.

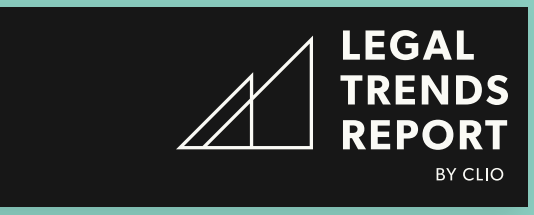
Data collection

- All data insights were obtained in strict accordance with Clio's Terms of Service (section 2.12).
- All extracted data was aggregated and anonymized.
- No personally identifiable information was used.
- No data belonging to any law firm's clients was used.

Reporting

Aggregate data has been generalized where necessary to avoid instances where individual firm data could be identified. For example, to avoid reporting data on a small town with only one law firm, which would implicate all of this town's data to this firm, we only report at country, state, and metropolitan levels.

Additionally, raw data sets will never be shared externally. Clio is effectively a tally counter for user interactions—much like stadiums use turnstiles to count visitors without collecting any personally identifiable information from their customers. Similarly, as users interact with the Clio platform they trigger usage signals we can count and aggregate into data sets. We can identify trends without collecting information that reveals anything specific about individual customers.



Clio, the leader in cloud-based legal technology, empowers lawyers to be both client-centered and firm-focused through a suite of cloud-based solutions, including legal practice management, client intake, and legal CRM software.

Clio has been transforming the industry for over a decade with 150,000 customers spanning 90 countries, and the approval of over 65 bar associations and law societies globally.

Clio continues to lead the industry with initiatives like the *Legal Trends Report* the Clio Cloud Conference, and the Clio Academic Access Program. Clio has been recognized as one of Canada's Best Managed Companies, and a Deloitte Fast 50 and Fast 500 company.

Clio®

Learn more at clio.com