# Troutman Pepper's Incidents + Investigations Practice


**Contact**

**Ron Raether**
ron.raether@troutman.com
949.622.2722

**Sadia Mirza**
sadia.mirza@trouman.com
949.622.2786

# Table of Contents

# Incidents + Investigations


Our Privacy + Cyber team extends the range of privacy and cyber services traditionally offered by law firms, drawing upon our unique combination of global expertise in keys areas such as privacy program creation and implementation, licensing, financing and M&A transactions, incident response, litigation, and regulatory investigations and enforcement.

Since 2005, we have led the response to hundreds of data security incidents, regulatory investigations, and data breach litigation, and we have helped to shape how companies respond when data incidents occur. We work with clients across a variety of industries, including technology, insurance, financial services, professional services, government bodies, law enforcement, life sciences and health care, energy, and telecom.

**Comprehensive Incident Response Services**

Our Incident Response (IR) attorneys lead clients through all phases of the incident prevention, response, and recovery processes. From the onset of ransomware, malware, wire transfer fraud, or other incidents to the regulatory and litigation maelstrom that may follow, we have led the response to thousands of security incidents involving some of the largest retail, health care, banking, and government agencies, which collectively have impacted more than 1 billion people. Our national team thoroughly understands the unique business, legal and technological nuances in this ever-evolving area, and has decades of experience guiding clients across all aspects of data privacy and security, including:

- developing incident response plans and workflows to help reduce the impact of a security incident;
- thoroughly testing procedures for responding to security incidents through our unique approach to tabletop exercise workshops; and
- handling all aspects of incident response, including the business pressures, regulatory enforcement and litigation firestorm that typically follows a security incident. We have led the response to hundreds of data security incidents, regulatory investigations, and data breach litigations since 2005.

Our team guides clients through every step of the incident response process, including engaging vendors to conduct a forensic investigation, coordinating initial crisis management communications, interfacing with law enforcement, advising on regulatory compliance issues, and assessing and complying with state and federal notification requirements and data governance standards. Importantly, we also act as a calming influence for the business, addressing goodwill issues and concerns to ensure a smooth and efficient resolution process.

### Incident Response Plans

Thorough preparation is the best defense to a cyberattack or other data security incident (and issues that may follow).

An incident response plan is a critical component of an effective information security program. At Troutman Pepper, we leverage our unique blend of expertise, experience, and innovative thinking to help clients develop a formal, focused, and coordinated approach to responding to an incident. We take into account each organization's unique mission, size, structure, and functions, tailoring our approach to fit their specific needs. We understand that no two incidents are exactly the same, and our response plans reflect this understanding. Our response plans provide a flexible roadmap for responding to security incidents in a timely and effective manner, while also protecting customers, clients, and the brand. Our commitment to customization, along with our deep understanding of the complexities of information security, sets us apart from other firms in this area.

## Tabletop Exercises

Companies must periodically test their incident response plans and critical staff through a functional simulated exercise known as a tabletop exercise. At Troutman Pepper, we take this process a step further. Our tabletop exercise workshop identifies and addresses any deficiencies in a company's response capabilities but also provides a unique, hands-on learning experience that sets us apart from other firms. .We offer practical, client-specific advice and skilled counsel to help companies anticipate and prepare for potential issues. This bespoke approach differentiates us from the marketplace.

Our team walks clients through simulated scenarios that challenge incident response capabilities in a variety of expected and unexpected ways. The workshop also enables our clients to:

- Build incident response instincts, define roles, and create channels for information and decision-making.
- Test the limits of the incident response plan to prepare for the unexpected.
- Facilitate discussions related to improving existing incident response procedures and information security programs.
- Better understand the incident response process with a trusted breach advisor, who will lead you through an actual incident. Create channels of communications that improve not just incident response, but also building the written information security program

## 24/7 Incident Response

**In the event of a suspected security incident, our response team can be reached at incident.response@troutman.com.**

As a trusted advisor, Troutman Pepper's attorneys are adept at helping businesses quickly understand and effectively communicate about complex issues related to data breaches and cybersecurity incidents. Our technical expertise, combined with our legal acumen, enables us to provide comprehensive but easy to understand guidance from the moment an incident is suspected. Businesses must immediately address an actual or suspected incident involving unauthorized access to confidential information in order to comply with applicable laws and regulations, and engaging experienced counsel at the onset is essential in order to maintain the attorney-client privilege and protect all potentially compromised data and related work product. We apply a tailored triage approach to each incident, working with forensic experts to assess the scope of the breach and its known or potential impact on its business units, employees and consumers, and to determine whether any notification requirements to consumers, state and federal regulatory authorities or the media have been triggered. We apply effective communication strategies to help clients get their arms around the range of issues unique to every incident, and leverage those lines of communication while leading clients through implementation of the most appropriate breach response plan.

Since 2005, hundreds of companies have chosen our team to guide them through incidents of unauthorized access to data and digital assets, phishing attacks, and ransomware. Our national breach response team provides comprehensive advice 24/7/365 in areas such as internal investigations, root-cause analyses, breach identification and response, individual and regulatory notice, regulatory investigations, and litigation.

## Regulatory Response

How a company managed its information security before an incident, and how it responded during the incident itself, directly impacts any ensuing regulatory investigations and enforcement actions. At any stage — before, during, or after an incident — we know how to best protect and position our clients to prevail in this high-stakes environment. Our regulatory team leverages their diverse skills and expertise to anticipate the likely course of an investigation and to develop solutions that streamline the investigation, from initiation through conclusion. As a result, we apply the proper scale and record building to match the level of scrutiny that may

be anticipated from regulators. This strategic positioning empowers our clients to effectively articulate the situation at hand and mount a robust defense.

Drawing from experience as former regulators in attorneys general offices, we also regularly handle state attorney general investigations and matters before state administrative bodies and federal agencies. Our work before the Federal Trade Commission, the Consumer Financial Protection Bureau, the U.S. Department of Health and Human Services Office for Civil Rights, insurance commissioners, and state attorneys general spans several decades.

- **State Attorneys General**

  Every state and territorial Attorney General is empowered with enforcing their respective jurisdictions' privacy and cyber security laws. With 50+ database breach notification and consumer protection statutes, and the rapid proliferation of consumer data protection acts, clients need counsel who can help navigate the ever-changing regulatory, cyber landscape. Our attorneys have decades of experience as former regulators in Attorneys General offices and consequently know firsthand how to successfully approach a variety of state investigations, having handled thousands of database breach incidents as government officials.

- **State Administrative Bodies**

  State statutes require companies to notify both Attorneys General and, depending on their business, their primary state regulators upon a data breach. The maze of state regulations for companies operating in more than one state is highly circuitous. State regulatory bodies such as insurance commissioners, state corporation commissions, and consumer protection boards, to name a few, are empowered to issue and enforce regulations. Our attorneys have extensive experience with such agencies and effectively assist clients by representing their interests before their respective administrative boards.

- **Federal Agencies**

  Federal agencies promulgate regulations in the cybersecurity and privacy arena in rapid fashion and often without the deliberation typical of the legislative process. Federal enforcement is complex and involves varied administrative processes. Clients therefore need experienced legal counsel who can navigate the intricacies of federal agency actions. Our attorneys have handled cases before the FTC, CFPB, and U.S. Department of Health and Human Services, among other agencies. We can help position clients for the most favorable outcome should they become subject to federal investigation.

## Litigation

Occasionally investigations proceed to litigation. When that happens, organizations need legal counsel who can vigorously defend their interests in court. Our national privacy and data security Litigation team works collaboratively with our Compliance, Incident Response, and Regulatory teams to provide clients with the expertise and resources needed to address the complex challenges they face with regard to their data management and information security. From the time we are engaged, our experienced litigators are available to assist clients with:

- Risk reduction advice;
- Strategies for protecting privilege and work product;
- Responding to requests for information;
- Preparing communications related to incident response; and

- Handling any litigation that may arise.

Our litigators have handled hundreds of litigations and arbitrations throughout the United States involving federal and state privacy statutory, tort, contract, UDTPA, and other theories that address the collection, security, use, and dissemination of personal information, including class action, single-plaintiff, and qui tam cases. Our experience includes representing diverse and heavily regulated businesses in financial services, health care and life sciences, education, energy, automotive, construction, education, and retail merchants for both controllers (businesses) and processors (service providers). It also includes representing businesses that deal in security, data aggregation and analytics, mobile applications, payment processing, de-identification/anonymization, correlation of data from multiple connected devices, and consumer-reporting systems.

We are also adept at advising on and representing clients in B-2-B privacy and data security disputes in connection with claims relating to breaches of contract and indemnification.

## Troutman Pepper Team


**Sadia Mirza, Partner**
Orange County
sadia.mirza@troutman.com
949.622.2786

**Stephen Piepgrass, Partner**
Richmond
stephen.piepgrass@troutman.com
804.697.1320

**Ron Raether, Partner**
Orange County
ron.raether@troutman.com
949.622.2722

**Ashley Taylor, Partner**
Richmond
ashley.taylor@troutman.com
804.697.1286

**Gene Fishel, Counsel**
Richmond
gene.fishel@troutman.com
804.697.1263

**Karla Ballesteros, Associate**
Orange County
karla.ballesteros@troutman.com
949.622.2415

**Robyn Lin, Associate**
Orange County
robyn.lin@troutman.com
949.622.2447

**Whitney Shephard, Associate**
Boston
whitney.shephard@troutman.com
617.443.3709

**Edgar Vargas, Associate**
Orange County
edgar.vargas@troutman.com
949.622.2473

# Recent Incident Response Thought Leadership

## Co-author, "Data Protection: One of These Incidents Is Not Like the Other," Reuters and Westlaw Today, August 24, 2023.

In the burgeoning realm of data incidents, it is a truism that such incidents are not created equal. Indeed, a data incident is not necessarily a data breach.
An incident is any "occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of an information system," or an event that constitutes a violation of an organization's computer security or acceptable use policies. National Institute of Standards and Technology, Minimum Security Requirements for Federal Information and Information Systems, FIPS 200, at 7 (Mar. 9, 2006) (nist.gov). A breach is an incident that imposes statutory and regulatory obligations on an affected organization when it holds or controls certain consumer information.

Data incidents and associated breaches can engender state and/or federal investigations, shareholder suits, and consumer-driven private litigation, including class actions. Organizations therefore must quickly assess the nature and scope of a data incident and undertake a course that not only resolves the incident itself but also addresses all legal obligations while simultaneously limiting liability exposure.

In part one of this four-part series, we identify the different types of incidents and what regulators look for when evaluating them.

**A. Three categories of incidents**
No two sets of facts are identical among data incidents, although many retain similar characteristics. Recognizing this, we can organize them into three broad categories: (1) those that are quickly assessed and contained, (2) those where the scope is uncertain and further investigation is necessary, and (3) those of such a large scale or sensitive nature, whether readily apparent or not, that a regulatory investigation is all but inevitable. Certainly, these categories are not mutually exclusive, as an incident can shift between them or encompass more than one.
Notably, the specter of government investigation hovers over each of these categorical baskets, particularly if the incident is, or potentially could be, a breach. Organizations must therefore be vigilant in the wake of any incident. Legal obligations, such as data breach notification statutes and agency regulations, are generally invoked when certain "personal identifying information," or an equivalent label, is compromised, thus transforming it into a breach.
Confusingly, each state and regulatory body has its own definition of personal identifying information. Social Security numbers, financial account information, and driver's license or state identification numbers generally trigger laws across the board. Information like date of birth, medical information, passport numbers, and biometric data, however, receive varied treatment. Given this, organizations should be aware that, depending on its size, an incident may enkindle federal regulations and/or 50+ state and territorial laws, and so should consult with legal counsel as appropriate.

**1. Quickly assessed and contained incidents**
These incidents typically involve an event that is smaller in scale and affects an easily identifiable data set. For example, a company employee accidentally emails a spreadsheet containing the names and credit card numbers of 100 of the company's customers to the wrong individual. The email provides clear evidence of what was sent and to whom.

Presumably, the risk of harm to the customers is relatively low particularly if the recipient is familiar and it can be confirmed the recipient quickly deleted the email. Yet this scenario may still be a breach in some states. If the company quickly addresses the incident and provides notice in a timely fashion, governmental entities are unlikely to initiate an investigation, presuming there are no other aggravating factors.

**2. Incidents of uncertain scope**
These are incidents requiring in-depth investigation to determine what data was affected, if any. In this hypothetical, an employee for a tax preparation service company inadvertently mails flash drives to 50 clients containing tax information pertaining to the company's employees. The company is unsure specifically what employee information is contained on each flash drive.
There is a chance, however, that any one drive contains an employee's Social Security number and the tax withheld from that employee's income. Importantly, if indeed present, these data elements qualify the incident as a breach under many states' breach notification statutes. It will be a challenge to track down all 50 flash drives and it will likely take the organization significant time to fully uncover the facts if they fully uncover them at all.

Ultimately, notice to affected consumers may be required once the incident is confirmed to be a breach. When assessing notification to regulators, businesses may want to consider a strategy at the incident's outset of ongoing communication with updates and developments as the matter evolves. Regulators often include state Attorneys General and/or a primary industry regulator such as a Commissioner of Insurance or State Corporation Commission.

**3. Large-scale and sensitive incidents**
Some incidents will most assuredly garner regulatory scrutiny. For example, a hacker infiltrates a health insurance company's network and exfiltrates the Social Security numbers and health diagnoses information for 15 million patients. She then appears to sell this information on the dark web.

This is clearly large-scale because of the number of affected patients, and it involves information that, while not protected by all breach notification statutes, may be viewed by consumers as "personal" nonetheless. This breach may draw the attention (and ire) of state Attorneys General that maintain jurisdiction as well as the company's primary insurance regulators.

In such scenarios an organization must steel itself for multiple and protracted investigations. Early and transparent communication with stakeholders as outlined below is essential.

**B. Regulator concerns and mitigation**
Within this universe of incidents then, what raises red flags for controlling government entities? Regulators look at several factors when deciding whether to pursue an investigation, including:

- The number of consumers affected,
- The consumer demographic affected (e.g., the elderly),
- The sensitivity of the data at issue,
- The likelihood of consumer harm,
- The type of intrusion,
- The applicable legal obligations,
- The amount of media attention,

- The affected organization's response, and
- The regulator's desire to make a broader policy statement.

Not all the above factors need be implicated to trigger regulatory scrutiny. Indeed, only one aggravation can suffice, or any combination thereof, for regulators to launch an inquiry.

Transparency and promptness in breach notifications help mitigate regulatory scrutiny and maintain consumer trust. Below are specific factors to consider when developing a pre-incident plan and navigating an incident.

**1. Pre-incident security safeguards**
Regulators routinely seek information about security measures and protocols in place before an incident. Establishing an information security program modeled after established frameworks such as the CIS Security Controls or the NIST Cybersecurity Framework demonstrate proactive measures taken to secure data.

Organizations should continuously adapt cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. See Nat'l Inst. of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (Apr. 16, 2019). They should also develop an incident response plan and conduct routine tabletop exercises to test the plan's efficacy. Such steps will positively reflect an organization's commitment to guarding against ever changing threats in the technological landscape.

**2. Timely and transparent communication**
Upon a breach, regulators focus on the timing of notifications to consumers and regulators. Each state's breach notification law dictates the timing of the notice. Some states require notice in as little as within 30 days after discovery of a breach. Others require notice "without unreasonable delay" after discovery, with reasonableness dependent on the type of breach, the investigation's length, the number of affected consumers, and the ease of identifying those consumers among other factors.

Transparency is also critical. Explaining the incident in general terms and what data was affected, if known, is necessary at the outset, and often required by law. A response should present clear information to affected individuals, along with sufficient self-help resources, like advice on contacting credit bureaus. Where needed, it should also indicate the method the organization will use to contact consumers with updates and a number to call for questions.

The responding party must also carefully discern between those facts that should be disclosed to comply with all pertinent laws from those "facts" that still may not be fully known and may also unnecessarily expose the organization to regulatory and litigative risk. Striking the right balance is essential to avoid further complications.

**3. Cooperation with regulators**
Organizations must proactively reach out to potential federal and state agencies that may retain jurisdiction over a breach when appropriate. This includes providing an explanation of the timeline from the incident's discovery to the date, or potential date, of notifications and issues that have arisen during the forensic process.

Further, regulators often look favorably upon early notification to law enforcement. Law enforcement may subsequently ask that notification to affected parties be delayed to not compromise the ongoing criminal investigation. Most state breach notification statutes allow for such a delay, but only if law enforcement has requested it.

Many state laws require affected organizations to list steps it will take to prevent future breaches. Detailing changes implemented such as improved security measures, enhanced protocols, and employee training, can demonstrate a committed path forward.

**4. Further response strengthening**
Regulators typically ensure organizations have executed a response plan throughout a breach and its aftermath. Organizations should coordinate responses with internal and external stakeholders, including deploying forensics with deliberate speed to identify, contain, and assess the incident. Other measures include, where relevant, confirming the extent of accessed or exfiltrated data, conducting dark web monitoring to verify leaked, exfiltrated data, and, for a ransomware attack, weighing a ransom payment with assurances from threat actors.
Organizations should consider offering at least a year of free credit monitoring or identity theft protection, which is required in some states. Finally, continually updating an organization's website with clear and concise language about the breach, along with establishing a call center or a website providing answers to frequently asked questions, reflects positively upon response efforts and will save time. See Fed. Trade Comm'n, Data Breach Response: A Guide for Business (Feb. 2021).

**Conclusion**
Incidents are not homogenous. By acting swiftly to identify their nature and contain them, take appropriate remedial measures, and notify pertinent parties, an organization can mitigate regulatory scrutiny and position itself for a quick recovery.

In part two of this series, we will cover the key regulators in the data incident arena and how they operate.

## Co-author, "Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter," *Reuters* and *Westlaw Today*, October 16, 2023.

Government regulators are seemingly as numerous as the stars nowadays, especially in the universe of data incidents. When organizations experience a data incident, they will need to quickly assess what happened, why it happened, and who (e.g., clients, consumers, vendors, employees) was affected. They will also need to chart a course by which they resolve the incident while limiting their legal exposure.

While they do so, they may attract the interest of regulators. As we discussed in part one of this series — "Data protection: One of these incidents is not like the other," Reuters Legal News and Westlaw Today, Aug. 24, 2023 — regulators take particular interest in a data breach when it involves sensitive data, a large number of consumers, or a vulnerable consumer demographic, among other factors. But who are these regulators? Here are the regulators most likely to come calling.

**State attorneys general**
State attorneys general play a significant role in regulating data incidents at the state level, as they usually enforce their respective states' data breach related laws. Indeed, every state has breach-related laws, including data breach notification statutes, personal information protection acts, data privacy laws, or consumer protection acts. Some states, like Connecticut, Florida, Indiana, Massachusetts, and Texas

are known for their particularly aggressive pursuit of breach matters. California stands alone with significant resources devoted to data regulation, including the relatively new California Privacy Protection Agency.

State AGs can impose fines and demand that organizations take corrective actions. Organizations that experience data breaches may end up facing multiple state AGs. Multistate involvement makes the regulatory landscape particularly complex, requiring careful coordination and compliance efforts.

To facilitate multistate investigations, state and territorial AGs often collaborate through the National Association of Attorneys General (NAAG). Breaches that are national in scope will often attract the attention of all 50 states, the District of Columbia, and U.S. territories. The AGs will then typically form an executive committee of two to seven states early in the process to lead the investigation, with the remaining states participating within a larger working group.
Whether a particular state AG takes a leadership role in an investigation often depends on where the organization that experienced the incident is headquartered, where it maintains significant operations, the number of impacted residents of a state, or the applicability of a state's laws in the context of the incident.

A multistate executive committee serves as the mouthpiece for the investigating states, which makes it easier from a practical standpoint for affected organizations to negotiate. The AGs within the working groups routinely meet among themselves to discuss ongoing investigations and strategize. With their collective goals in mind, executive committee member states will issue civil investigative demands and subpoenas to a subject organization, and seek to engage the affected organization's counsel, which may lead to settlement negotiations.

Although they coordinate investigations, every state AG has its own nuanced legal requirements, policy agenda, and even personality that organizations must navigate to effectuate a satisfactory resolution. And occasionally states will disagree on the best approach, leading some to break away from the multistate group and, as sovereign entities, commence their own investigations. Handling an investigation can therefore take months or years to resolve, particularly where large AG working groups are involved or where parallel state investigations are opened.

**Federal agencies**
Besides state AGs, many federal administrative agencies may respond to data breaches.
To safeguard consumer data, the Federal Trade Commission (FTC) enforces various laws, including the Federal Trade Commission Act and the Health Breach Notification Rule. Upon a data incident, the FTC often investigates an organization's data security practices, incident response plan, and breach notification procedures. If the FTC believes an organization's actions (or inaction) contributed to the incident, it can mandate implementation of robust security measures and impose hefty fines if an organization fails to comply.

The U.S. Department of Health and Human Services (HHS), through its Office for Civil Rights (OCR), investigates breaches of protected health information (PHI), and may coordinate its investigation with state AGs, who also retain power under HIPAA (Health Insurance Portability and Accountability Act). When a health care entity suffers a PHI breach, it may need to report it to HHS and affected individuals. Depending on the severity of an incident and the extent of an organization's non-compliance, HHS can impose civil penalties and require corrective action to prevent future incidents and breaches.

The Securities and Exchange Commission (SEC) may investigate when a data incident affects a publicly traded company, as public companies must now (as of July 2023) disclose any "material" cybersecurity incident within four business days. Companies must disclose the material aspects of the incident and any material or potentially material impact on the company.

The Federal Communications Commission (FCC) investigates data incidents that affect internet and telecommunications services. The FCC's Privacy and Data Protection Task Force has been tasked with strengthening the FCC's rules for when and how internet and telecommunication providers notify consumers and federal law enforcement about data incidents.

Several other federal agencies, including the Department of Transportation, Federal Aviation Administration, and the Department of Education may also inquire in the wake of a breach that affects entities within their purview.

**Law enforcement agencies**
In contrast to civil investigative authorities, law enforcement agencies may open criminal investigations into data incidents. Factors that prompt criminal investigation include the egregiousness of the incident and the amount of loss suffered by victims. Law enforcement goals include bringing a perpetrator to justice, protecting the public, and deterring future criminal conduct.

Both state and federal law enforcement agencies retain jurisdiction over data breaches and investigate under criminal statutes prohibiting fraud, hacking, and espionage among others. Such agencies may issue subpoenas and search warrants for computers that an affected organization maintains.

On the federal side, the Federal Bureau of Investigation (FBI) is highly active in investigating large-scale breaches. The United States Secret Service investigates breaches that involve financial transactions. And the Department of Homeland Security may investigate breaches with an international scope. Regardless of the federal investigating agency, if the investigation develops into criminal charges, the Department of Justice (DOJ), often through local U.S. Attorneys' Offices, will handle the resulting prosecution in federal court.

As a general rule, investigating agencies will often try to minimize the impact on business operations when executing criminal processes, particularly if the organization is not criminally at fault. This said, representatives of affected organizations should not necessarily mistake law enforcement deference for aligned interests. Beyond mandatory compliance with criminal process, organizations that cooperate with law enforcement must be careful to not disclose certain privileged information. Thus, organizations would be well-advised to consult legal counsel before talking to law enforcement.

**Other players**
Some industry-specific state administrative agencies also may maintain jurisdiction over a data breach if a breached organization falls within their purview. For instance, state insurance bureaus may investigate a breach of an insurance company if they act as that company's primary regulator. Additionally, if a financial institution suffers an incident, various states' divisions of banking or finance may initiate investigations. But because state AGs often have more statutory weapons in their arsenal, they typically serve as a state's lead investigating agency, unless they are statutorily divested of jurisdiction via a grant of primary authority to another state administrative agency.

On the international front, a significant cross-border data breach will likely garner scrutiny from multiple international data protection authorities especially in the European Union, United Kingdom, China, and Mexico. International law enforcement agencies such as Interpol and the Royal Mounted Canadian Police may also initiate investigations. An organization's counsel in the United States should therefore work closely with international counsel versed in the pertinent country's laws to address overlapping issues and privilege concerns.

Finally, organizations must always be cognizant of potential class actions and multidistrict litigation. If a data incident is large enough, plaintiffs' firms may seek to quickly file such actions in its wake. Information is not always shared between regulators conducting investigations and plaintiff's counsel pursuing parallel class actions, but organizations need experienced counsel who can balance confidentiality issues and cross-litigative risks as they negotiate these multiple paths forward.

**The regulators are interested in talking; now what?**
Navigating the labyrinth of federal and state regulators in the wake of a data incident has become increasingly complex over the past two decades. Organizations must strike a balance between cooperation and self-preservation. Each regulator requires a unique approach that should be grounded in institutional knowledge and experience. Therefore, an organization must consult with experienced counsel early and often to favorably position itself relative to regulators.

Once lines of communication are established between an affected organization and an investigating regulator, several factors will determine a successful resolution. In part three of this four-part series, we will discuss these factors in detail and map out a successful strategy for handling data breach investigations.

### Co-author, "A Checklist for Cyber Incident Response Communications," *Law360*, July 14, 2023.

Popular file transfer tool MOVEit's recent data security vulnerability prompted many businesses to communicate, internally and externally, about the impact of the incident on its business.

Businesses from various industries — including insurance, finance, government, health care, education, professional services, media and entertainment, and software providers — adopted different messaging approaches in terms of timing, transparency and content.

This serves as a reminder that there is no one-size-fits-all approach to incident response communications.

While there is no single strategy that will work for all businesses or all incidents, there are certain questions that every business should ask before communicating about an incident.

These questions, when considered, help ensure that any messaging will not further expose the organization to legal and business risks, and instead improve the narrative around its response.

**Is the timing right?**

When dealing with a security incident, it is good to consider the story that will be told about the business's response.

One storyline that is often favorable is that the business notified affected individuals or customers as soon as possible.

With that said, organizations need to balance the need, or desire, to quickly inform affected parties of the incident with ensuring that there is enough information to answer the questions that will inherently come up.

These questions may include: What information was affected? What was the root cause? Has the incident been contained?

Thus, in certain circumstances, the ideal situation may be providing notice only after the investigation is complete.

Businesses, however, may not always have the luxury to wait, as certain situations may warrant notice sooner. For example, if the incident has already been published in the media, or customers are aware that services are down or have been affected, a business may be forced to address the incident head on, even while the investigation is ongoing.

Likewise, there may be contractual or legal notification obligations that trigger a notification requirement. Or, as with the MOVEit incident, businesses may need to notify third parties because there is a need to take immediate action — e.g., patch a zero-day vulnerability.

Regardless of when the business decides to notify, it needs to keep its story in mind. Companies should be prepared to explain their timeline from the discovery of the incident up to the point of notification.

One narrative to consider, which arguably aligns with breach notification laws, is that providing notice too soon — when there was not enough information about the nature or scope of the incident — would cause unnecessary panic and result in over notification. Thus, the business took its time to conduct a reasonable investigation to ensure it understood the incident instead of rushing to provide notice.

Alternatively, when notice is provided at the onset of an incident, a business should use that fact to its advantage.

While there may be challenging conversations to be had about the incident at that time, the business will ultimately be able to walk away saying that it provided notice as quickly as possible in the interest of being transparent and forthcoming.

**Has the business prepared for the follow-up?**

Assume the company has decided to provide notice of the incident. Has it, however, thought through the follow-up?

Businesses should read their messaging through the eyes of consumers, customers and regulators. What questions would they ask, and what communication protocol can the business implement to address them now?

If notice is being provided during an ongoing investigation, it is likely there will be questions relating to containment and ongoing risk. For example, customers may question whether it is safe to resume business with the organization during an ongoing investigation.

Businesses should consider what assurances they can provide if the question comes up, and what can be done from a containment perspective to mitigate these concerns.

A layered-notice approach is one strategy to consider when notice is provided during an ongoing investigation. This strategy offers initial, high-level information about the incident suitable for a broader audience.

For consumers or customers with specific follow-up questions, a second notice is prepared in advance, providing additional factual details. By having a second notice ready to go, businesses can quickly respond to any follow-up, allowing them to focus their efforts on where it is most needed — the ongoing investigation.

The second notice also provides the added benefit of making consumers and customers feel that businesses are being transparent about the incident, or that they are part of the solution.

If notice is being provided once the investigation is complete, consumers and customers may ask specific questions about the impact of the incident on their data and the resources that are being offered to assist.

This is typically when businesses will create FAQs and line up a dedicated call center to answer common questions. There should also be an established escalation plan — including escalation contact — to address those questions that were not covered by the FAQs.

**Is the messaging factual, and does it avoid speculation?**

As with forensic reports, messaging during incident response should be factual.

Businesses should avoid providing opinions or speculating as to the impact of the incident or its root cause, especially when an incident is still under investigation.

Often, speculation results in businesses needing to correct prior statements made. This keeps the incident fresh in consumers and customers' minds, making it difficult for the company to move past it.

While a company wants to minimize the impact of the incident, it is important the company does not describe the incident in a manner that would deter affected parties from taking certain precautionary steps.

For example, even if the business conducted dark web monitoring to ensure that data has not been leaked, this should not be in stated in a way to suggest that there is no need to sign up for any credit monitoring being offered.

Ultimately, affected parties should always be encouraged to take steps to protect their data, and it should be up to them to decide whether there is no risk based on the facts, not opinions, provided.

**Does the messaging provide sufficient context?**

A central goal of messaging should be to minimize the impact of the incident on the business.

To help achieve that goal, a business should provide adequate context to any message. What constitutes sufficient context will of course depend on the specific situation, but there are certain questions a business can consider to help ensure the message provides sufficient context.

One question to consider is: Where did the incident occur?

Suppose the business is providing notice about an incident that affected one of its third-party service providers. In that case, explaining the relationship between the business and that third party is imperative.

Otherwise, message recipients may ignore the message, wrongly assuming it does not apply to them because they have never done business with that third party or fail to focus on the message contents. They will instead be too focused on trying to understand how the business and third party are related, or why the third party has their personal information.

Another question to consider is whether to explain the type of incident. Explaining to the message recipients the type of incident — a phishing campaign, a fraudulent wire transfer, a ransomware event — can help manage the recipients' expectations.

Knowing that the business fell victim to a phishing campaign during which an unauthorized party accessed the business's email environment to send out phishing links will likely elicit a different response than a message indicating that a business experienced a ransomware attack.

When relaying the nature of the incident, however, businesses should consider the demographics of their audience, including their ages and locale. For less technically savvy audiences, avoiding legal or technical jargon is important to ensure the message does not get lost in translation.

Businesses should also consider whether additional context is needed to explain any calls to action. For example, if a company asks customers to apply patches to their software, providing context as to why the patch is needed may be critical to ensure customers follow through quickly.

Likewise, if a company recommended individuals change their passwords for accounts unrelated to its system, explaining the concept of "password reuse" may quell consumers' fear of how far spread the impact of the incident is.

**Can the business take additional steps to minimize potential risks and concerns?**

Many businesses tend to wait until their investigation is finished before suggesting protective and preventive measures.

However, it may be beneficial to consider taking action or providing support during the investigation to reduce the negative impact of the incident on the company.

One scenario where this may be prudent is when an organization experiences a ransomware attack, and the business suspects that employee information has been affected. In such a scenario, offering employees and their dependents family credit monitoring while the incident investigation is ongoing may allay, if not altogether quell, employee concerns.

Consider also when an organization learns it has been the victim of wire fraud. The initial impulse may be to remain silent and only notify other businesses if those businesses sent payment to the fraudulent account.

It may behoove a business, however, to let all its customers know, while the investigation is pending, not to send any wire payments without first confirming the correct account information. Doing so may prevent another organization from sending payment to the wrong address.

**Has the business considered the audience?**

The above questions are important to consider before issuing any message about an incident.

While the focus has primarily been on the message itself — the timing, transparency and content — it is equally important to consider the intended, and unintended, recipients of the message.

If messaging internally, consider how employees will respond to the message. Are they likely to keep the information confidential, or is there a chance that it may be shared with a broader audience?

The answer to this question may dictate how much information is shared about the incident and when.

If messaging externally, consider how customers and clients will respond. Is the customer likely to be understanding and receptive to the situation? Or is it possible the customer will cease business operations until their demands are satisfied?

The answers to these questions may vary depending on the sophistication level of a company's customers. It may be prudent to prepare specific communications for the VIP customers who require more hand-holding than others.

It is important to keep in mind that if notice is given, the media may become involved. Therefore, it is essential to have a media statement prepared in advance that aligns with other communication efforts as part of a comprehensive communication strategy.

Lastly, keep in mind that a company's messages may be reviewed by regulators and plaintiffs lawyers at some point. It's important to review messages with this in mind to ensure that even well-intentioned statements won't be used against a company in the event of litigation or an investigation.

### Co-author, "January 2023 Tech Tip - How to Know if You Should Consult a Breach Coach," *Orange County Bar Association*, January 10, 2023.

Some companies consider investing in cybersecurity as an unnecessary business expense. Lawyers are often viewed as an unnecessary business expense, too. So, it is no surprise that when companies experience a "data breach" they often resist hiring a cybersecurity attorney to help.

Why should a company hire an attorney while experiencing a data breach? The answer is simple: a breach coach's role is to solve problems and help navigate the company's response. More often than not, by hiring a breach coach, an organization experiencing a data breach will minimize its legal and business costs.

Before discussing ways a breach coach helps, it is important to define it. At a high-level, a "breach coach" is a cybersecurity attorney who provides legal counsel to an organization experiencing a data incident. While the guidance provided will undoubtedly depend on the nature of the data incident, a breach coach assesses the data incident and devises a response strategy. The end goal is to minimize the data incident's legal and business impact on the company.

**Breach Notification Requirements**

You may have noticed the nomenclature switch from "data breach" to "data incident." That is intentional. Not all data incidents are data breaches; a breach coach determines if the company's incident is just an incident or if it is a data breach. A data breach imposes statutory and potentially regulatory obligations on an organization. A data incident does not. If a breach coach determines a breach occurred, the breach coach will identify the company's resulting legal and regulatory notification obligations and comply with them on the company's behalf.

Legal concerns may not be limited to statutory and regulatory notification obligations, however. Some companies have contractual notification requirements that trigger when a data incident is suspected. A breach coach identifies the company's contractual notification requirements and complies with them.

A company responding to data incidents without a breach coach tends to over-notify, telling everyone that the company experienced a breach, or under-notify, telling no one. Neither outcome is ideal. If a company over-notifies, it may have unnecessarily reported to consumers, increasing the likelihood of a data breach class action in the process. And, while a company that under-notifies may reduce the likelihood of a data breach class action, it may have run afoul of statutory and regulatory notification requirements, and consequently, exposed the company to regulatory fines.

**Assigning Responsibility After a Fraudulent Wire Transfer**

The legal ramifications following a data security incident are not always limited to assessing and complying with notification obligations. Sometimes a data security incident involves a scheme whereby an unknown threat actor imputes himself into an email exchange between a company and the company's vendor and poses as the vendor. The threat actor then emails the company new payment instructions. As a result, the company pays the threat actor instead of the vendor, leaving an unpaid vendor demanding payment from a company that is already out the money it owes the vendor.

Resolving such a scenario can be problematic, especially if the company and vendor intend to continue their business relationship. Engaging a breach coach, however, can help a company reach a resolution. One way a breach coach can help is by engaging a third-party on the company's behalf to conduct a privileged forensic investigation. The investigation's goal is to determine if the threat actor entered the company's email environment or the vendor's. Knowing how the threat actor was able to intercept the email exchange carries significant import in resolving these types of disputes.

**Business Concerns: Determining the Cause and Messaging Stakeholders**

The importance of learning how (or if) a threat actor entered a company's network extends beyond the fraudulent wire transfer context. When a company experiences a data security incident, the company is often more concerned about minimizing business interruption than identifying and satisfying statutory and regulatory notification requirements. A breach coach understands that a data incident impacts an organization from both a business and legal perspective.

One way to minimize business interruption is to restore the impacted business to normal operations as soon as possible. To expedite a return to normal, a company will often "wipe" all computers and servers the threat actor accessed—so that they are "clean"—and put them back on the network. But the threat actor may still be in the network, and simply putting "clean" devices back on a "dirty" network will render those devices dirty once again. Possibly worse, a well-intentioned IT provider may wipe the impacted devices before preserving a copy of them, destroying valuable forensic evidence.

Two common questions an impacted organization experiencing a data incident is asked, from both internal and external stakeholders, will cover: (i) how this happened and (ii) what the company is doing to prevent this from happening again.

A breach coach can help provide answers to these questions, usually by facilitating a privileged investigation. Privilege is especially critical in this context since sometimes the answers are not favorable (e.g., the incident occurred because the company did not have appropriate security protocols in place). A breach coach can help deliver that message in a way that limits regulatory scrutiny and potential legal liability. And, while a breach coach determines from a legal standpoint who must receive notification, a breach coach can also recommend whom you could and whom you should notify— from a business standpoint.

There are many ways a breach coach can help a company before an incident even occurs, but in the meantime, we will leave you with the following thoughts.

**Situations in Which You Might Need a Breach Coach**

1. You suspect a security incident.
2. You don't know the difference between a "data incident" and a "data breach."
3. You don't know that "breach" is a legally defined term and that its definition varies depending on the law of the applicable jurisdiction.
4. You don't have an incident response plan.
5. You've never experienced (or at least believe you've never experienced) a security incident.
6. You don't know what a forensic investigation is or why it may be needed.
7. You don't know if your company should conduct a forensic investigation following an incident.
8. You don't know how to contact law enforcement to report an incident.
9. You don't know any forensic vendors.
10. You don't know if you must notify anyone following an incident.
11. You don't know if you should notify anyone following an incident.
12. You don't know what to say in your breach notification.
13. You don't know what your company would do if hit with a ransomware attack.
14. You don't know where to obtain bitcoin.
15. You don't know how to conduct an OFAC check.
16. You want to take steps to reduce the chances of experiencing a data incident.

Let's face it, cybersecurity and the cybersecurity legal landscape can be complicated to the uninitiated. If your company experiences, or believes it has experienced, a data incident, contact a breach coach. The breach coach can recommend what to do in response based on prior experience.

**Co-author, "Forensic Artifacts Play Legal Role in Cyber Incident Response," *Law360*, December 2, 2022.**

When a business experiences a data security incident, there is invariably one principal question that the affected business wants answered: Who do we tell?

While this is a simple question, the answer is not. Ideally, after an incident, an affected business can decide whom it: (1) must tell about the incident; and (2) should tell about the incident. The first decision is a legal one. The second is a business decision.

After an incident, however, an affected business often does not have enough information to make these decisions.

**Forensic Artifacts: A Business and Legal Issue**

Enter forensic artifacts. In the context of incident response, forensic artifacts help explain what happened during the incident. These include things like registry keys, IP addresses, files, timestamps and event logs — things that help piece together the nature and scope of the incident.

Forensic artifacts serve both legal and business purposes. They answer questions such as:

- What was the root cause of the incident?
- When did the incident occur?
- What data was affected?
- Where should the business focus its containment and remediation efforts?

From a business perspective, the answers to these questions may assist the business with restoring affected systems, restoring altered or corrupted data needed for business critical functionality, preventing further damage to other systems, and improving the overall information security protocols.

From a legal perspective, the answer to these questions may help defend against potential claims, determine whether contractual requirements have been triggered, assist with identifying possible resolution options in a dispute and, critically, determine who the business must and should tell about the incident.

Legal teams often do not appreciate the legal purpose of forensic artifacts until it's too late. Instead, forensic artifacts are viewed as a security issue — resulting in legal teams having no input into what forensic artifacts a business should collect, and how long the business should retain them.

Understanding how forensic artifacts may save a business from declaring an incident as a data breach is critical, and should incentivize security and legal teams to work together before an incident occurs, to ensure they are positioning the business in the best way possible.

**Log and Tell: Business Email Compromise Example**

To better explain the legal role of forensic artifacts, consider what happens in a business email compromise, or BEC, attack. Who a business must tell generally depends on whether there is evidence of unauthorized access or acquisition of personal information — i.e., whether the incident qualifies as a data breach.

If a business has its full complement of logs, that business may be able to determine if the threat actor accessed or acquired personal information from the email environment and the specific files that the threat actor accessed or removed.

Without a full complement of logs, the business may not be able to determine if there is unauthorized access or acquisition of personal information — or the scope of unauthorized access or acquisition.

To assess a business's statutory notification obligations, it is critical to determine which emails the threat actor accessed or acquired. Not knowing the scope of an incident creates uncertainty. Does the affected business have to notify anyone about the incident, absent conclusive evidence of unauthorized access or acquisition of personal information?

In such a scenario, the affected business may find itself with two potentially unfavorable options: (1) Assume the worst-case scenario, namely, that all its customers' and employees' personal information has been subject to unauthorized access or acquisition, and notify everyone; or (2), assume none of its customers' and employees' personal information has been affected, and notify no one. Both scenarios pose unique risks from the litigation and regulatory perspectives.

Logs are also important in ransomware attacks. Firewall logs provide insight into the scope and timing of data exfiltration. VPN logs can provide insight into when and from where the threat actor accessed the environment.

Having this information available after an incident may be able to narrow the scope of the incident, possibly resulting in a smaller notification population.

**Legal and Security Teams Need to Work Together**

Drawing on our combined legal and security backgrounds, we compiled a comprehensive list of artifacts that forensic analysts typically request following a BEC incident or ransomware attack.

Different logs provide different information, and have varied retention periods. Legal and security teams should discuss what logs a business should retain, and for how long.

If an organization that uses Office 365 experiences a BEC incident, there are a bevy of logs that can provide insight into the incident itself and the organization's response to it. Microsoft Purview audit logs provide insight into user logins, mailbox activity, SharePoint/OneDrive file access or downloads, and other Office 365 network related activity. The standard retention period for them is 90 days.

Admin audit logs record actions by global administrators, record cmdlets executed and objects affected. These logs have a 90-day standard retention period. Mailbox search terms provide insight into what information an unauthorized user was searching for — i.e., "wire," "wire transfer," "bank information," etc.

Inbox and forwarding rules provide insight into whether the threat actor sent emails outside the business's email environment. Message trace logs provide a high-level metadata report of all incoming or outgoing emails for a specific user. These logs have a 90-day retention period.

A compromised user mailbox file allows an analyst to view a business email inbox as the legitimate user would. It therefore aids in viewing potential phishing emails, and understanding the regular use patterns of the user.

If an organization that uses Google Workspace experiences a BEC, Google Workspace has logs that retain certain information too. Audit logs provide insight into user logins, mailbox activity, Google Drive file access or downloads, and other network related activity. The standard retention period for these logs is six months.

User reports may show the last IMAP/POP3 login, the last web-based login, and password length, and provide other account status checks. These logs are retained for six months.

Mailbox search terms from Google Workspace also provide insight into what information an unauthorized user was searching for. Inbox and forwarding rules provide insight into whether the threat actor sent emails outside the business's email environment.

Email search logs provide a high-level metadata report of all incoming or outgoing emails for a specific user. These logs are retained for 30 days, and are similar to message trace logs in Office 365.

Google Vault allows an analyst to view a compromised user mailbox as the legitimate user would. It therefore aids in viewing potential phishing emails, and understanding the regular use patterns of the user.

Logs are also instructive in ransomware incidents. Firewall logs and admin console access monitor access into and out of the environment, including IP addresses, and the size or number of bytes being transferred in and out of the network. And VPN activity logs provide session history and length, IP addresses used by network protocols or user agents, and network bandwidth usage.

**Conclusion**

While these artifacts are useful in understanding what happened after an incident, it is important to discuss logging and retention long before an incident occurs. Legal and security teams should be aligned on their approach before, during and after an incident.

**Co-author, "**Focusing on the Primary Purpose: Protecting the Attorney–Client Privilege and Work Product Doctrine in Incident Response**,"** ***Cyber Security: A Peer-Reviewed Journal*****, July 11, 2022.**

**Abstract** Organizations responding to cyber security incidents must manage their incident response efforts while maintaining two critical legal protections: the attorney–client privilege and the work product doctrine. This paper analyses how the attorney–client privilege and the work product doctrine, when properly maintained, prevent information regarding an organization's thoughts and discussions from being disclosed or used in subsequent proceedings. It discusses how recent judicial decisions analyzing the application of these two doctrines have emphasized the importance of seemingly minor details that may

be overlooked during incident response efforts that can have significant consequences in subsequent legal actions when asserting protections. In particular, courts will focus on the stated purpose for any step in the incident response process (e.g., business versus legal), and any discrepancies between the stated purpose and conduct can have disastrous effects on future claims of protection in legal proceedings. This paper puts forward that organizations should craft incident response plans with the maintenance of these protections in mind. Practical steps organizations can take include carefully scrutinizing the language in retainer agreements, involving in-house or outside counsel at the earliest opportunity, limiting the disclosure of privileged materials, and exercising caution when documenting during incident response. After-the-fact attempts to shield the results of any investigation from opposing parties in litigation are rarely successful, so organizations should take affirmative steps to ensure the vitality of these two critical legal protections from the earliest stages of incident response, which start with the planning and preparation.

'In anticipation of litigation' — a phrase of only four words — is a term of art that can have pivotal consequences for companies of a growing trend. Minute details that can get lost in the chaotic shuffle following a cyber security incident can re-emerge years later to have profound effects. A few words in a retainer agreement can factor into whether investigatory findings can be limited to internal consideration — and thus shielded from being used against the target by opponents in the courtroom — and permitting candid conversations without fear that third parties will second-guess every choice or word used as parties work to defend against criminal hackers.

During a cyber security incident, companies must handle internal and external pressure to quickly answer fundamental questions, such as how the attack happened, is the incident contained, what information was affected and is notice required? While breach notification laws are structured to allow companies a reasonable time to investigate the incident, businesses often want to inform external parties of the incident immediately, without fully knowing what is at stake. This desire increases when the incident is detected by a third party (as opposed to the company itself), and the media and customers are already aware that an event occurred or is taking place.

These necessities often result in a perceived need for instant action and external communication. But this understandable need to move quickly can obfuscate and often conflict with critical, long-term considerations. One of these long-term concerns is protection of the attorney–client privilege and the work product doctrine. The pitfalls of failing to consider these protections can be drastic, but they are often slow to emerge, sometimes taking years to fully develop. By the time it is apparent that steps were not taken to preserve protections, it is often far too late to rectify the situation.

In most courts, whether protections apply depends on the court's assessment of the 'primary purpose' of the investigation.[1] For example, is the primary purpose to determine whether a threat is active, which may not be considered legal advice, or is the purpose to determine the root cause of the incident to assist counsel in defending against legal claims? In incident response, the practical reality is that an investigation may have overlapping purposes, but only an investigation with a predominantly legal purpose will receive protections. Companies affected by cyber security incidents, however, can take steps to shape how a court will assess the primary purpose of its incident response (IR) efforts, and companies should be mindful that preserving the vitality of these protections starts even before the incident occurs.

## AN OVERVIEW OF THE ATTORNEY– CLIENT PRIVILEGE AND THE WORK PRODUCT DOCTRINE

The attorney–client privilege and the work product doctrine are two related but distinct doctrines to protect information that is shared with legal counsel from future disclosure. The attorney–client privilege protects

communications to and from one's attorney(s) (and their delegates) for the purpose of seeking legal advice, while the work product doctrine protects materials prepared by an attorney — or the agents of an attorney — in anticipation of litigation. In the context of cyber security investigations, these two protections often overlap. Some people tend to group them together and treat them interchangeably, but the distinct purposes, origins and tests for these two protections inform the unique methods that must be employed to assert them during the life of cyber investigations and any subsequent litigation.

**Attorney–client privilege**

'The attorney–client privilege is the oldest of the privileges from confidential communication known to the common law.'[2] The privilege protects communications made to one's attorney for the purpose of seeking or obtaining legal advice, but it does not automatically attach to every communication between an attorney and a client. The Supreme Court noted the limitations of the privilege in Fisher v. United States:

> *'[S]ince the privilege has the effect of withholding relevant information from the factfinder, it applies only where necessary to achieve its purpose. Accordingly[,] it protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege.'*[3]

*To determine whether the attorney–client privilege applies to a given communication, courts will examine the motivation and purpose underlying the communication. In practical terms, however, courts will look beyond the confines of a single communication and examine the predominant purpose of the relationship that led to the communication.*[4] *Communications — even those to an attorney — that take place in the context of seeking business or technical advice likely will not fall under the privilege's protections, even if potential legal implications are discussed. And documents are not privileged merely because they are transmitted to an attorney. If that were the case, companies could withhold communications on the basis of attorney– client privilege simply by including their attorney on the communication.*[5]

**Work product doctrine**

*While the attorney–client privilege protects communications between a client and its attorneys, the work product doctrine protects documents produced by an attorney in preparation for litigation.*

*'At its core, the work product doctrine shelters the mental processes of the attorney, providing a privileged area within which the attorney can analyze and prepare his client's case.'*[6]
The doctrine protects not just materials prepared by the attorney, but those prepared by 'investigators and other agents' for the attorney's use.[7] This may include the attorney's notes, research files, or other information collected or prepared in anticipation of litigation.

The phrase 'in anticipation of litigation' is the critical determinant of whether the work product doctrine protects information developed.[8] This is effectively a 'because of' test. The doctrine only protects documents or information that would not have been developed but for the good-faith belief that it was necessary to do so because of pending or threatened litigation.[9] This inquiry has objective and subjective elements. Objectively, the party asserting the doctrine's protection must demonstrate that it had a reasonable belief a specific litigation threat existed. A general fear of litigation, not tied to a specific claim, is not enough.[10] But litigation need not be ongoing at the time of a document's creation for it to be made 'because of' litigation. For instance, while a government investigation itself is not litigation, courts have generally found that a government investigation gives a company a reasonable basis to anticipate

litigation. Subpoenas, requests for mediation, or even the nature and severity of the incident itself can all create a reasonable basis to anticipate litigation.[11] Courts will also examine a company's efforts to preserve potentially relevant documents — a duty also triggered by a reasonable anticipation of litigation — as evidence of whether a reasonable basis to anticipate litigation existed for work product purposes.[12] A company that plans to rely on work product protections for elements of its IR plan should plan to issue litigation holds simultaneously, both to comply with the duty to preserve evidence and to reinforce the existence of a reasonable basis to anticipate litigation.

Subjectively, the anticipated litigation must motivate the production of the document or information. Even with a reasonable and specific threat of litigation, a document that would have been prepared regardless of the threatened litigation will not receive work product protections.[13] Investigations conducted pursuant to regulatory requirement or internal policy are not created 'because of' litigation, even where litigation is anticipated. The party asserting work product protection over a particular document has the burden of showing that the protection applies, including demonstrating that the material was prepared in anticipation of litigation.[14]

The attorney–client privilege and the work product doctrine are valuable tools that can protect information which, if shared, may be harmful to a company's defense should a regulatory investigation or lawsuit ensue. In practice, courts examine similar factors in applying both the attorney–client privilege and the work product doctrine. The focus is always on the primary purpose and motive of the communication. If the court finds that the primary purpose is driven from a legal necessity (as opposed to a business need), it is more likely to find the material to be protected.

## BOLSTERING AN ARGUMENT THAT PROTECTIONS APPLY

Recent judicial decisions have reaffirmed that establishing protections involves a highly fact-sensitive inquiry. What is clear, however, is that whether a document or communication can be shielded from prying eyes depends on its purpose, and whether the actions that follow align with the declared purpose. While seemingly straightforward, the practical reality is that actions taken as part of incident response efforts often serve dual purposes (e.g., a business purpose and a legal purpose). Consider, for example, an organization's need to identify potentially affected data following an incident. From a business perspective, this information may be needed to fix corrupted or altered data to support product functionality. From a legal perspective, this same information is needed as it informs an organization's legal notice requirements. But only this latter (legal) purpose stands a chance of being protected by the attorney–client privilege. Similarly, an estimate of the number of affected users serves a business purpose to help craft a public relations strategy. Counsel may also request a similar estimate to predict the size of a class action lawsuit after litigation is threatened. But only documents created because of the threatened litigation will receive work product protection. Whether determining the primary purpose of a communication or if a document was created because of a litigation threat, courts will examine the stated purpose, conduct and result of any action to determine whether they align with the claimed protections.

No fixed formula will ensure protections apply. Rather, following proper procedure provides the best shot to establish the attorney–client privilege and work product doctrine, but companies would be wise to proceed with caution. Indeed, courts appear to be ruling, more often than not, that responding to an incident is primarily a business function. Despite this trend, some organizations have been successful in shielding IR documents. Drawing from these examples, the following are a few steps businesses can take to bolster an argument that protections apply.

**At the first sign of an incident: Engage in-house counsel**

Not all cyber security incidents require the same response or lead to the same outcomes. And of course, not all cyber security incidents will result in litigation. Businesses and incident response teams, however, have not historically been good at discerning which incidents will result in litigation and/or investigation, thus often resulting in organizations skipping steps that are critical to preserve protections. Thus, at the first sign of an incident, organizations should engage in-house counsel immediately for two critical reasons. First, by involving in-house counsel, companies may be able to demonstrate that their IR efforts were driven from a legal necessity (e.g., a belief that litigation is reasonably anticipated and thus counsel should be involved). Secondly, in-house counsel may be in a better position to assess whether retaining outside counsel is necessary after assessing the potential magnitude and impact of the incident. Factors the legal team may take into consideration when determining an appropriate response to an incident and potential outcome include the number of consumers/customers affected, types of data at issue (eg personally identifiable information and protected health information), the likelihood of harm to individuals, type of intrusion, the privacy and data security laws/contractual obligations applicable to the organization, and the amount of media attention the incident is receiving.

Of course, not every incident will warrant bringing in outside counsel. The in-house legal team, or counsel serving this function, however, is likely in the best position to make this determination. For organizations that do not have an in-house counsel legal team, or someone experienced to conduct this evaluation, it would be wise to have a plan in place to ensure this step is not overlooked. One option is to obtain cyber insurance so that in the event of an incident, the carrier can connect the company with counsel experienced in this area of the law.

**When the situation warrants it: Hire outside counsel**

Reliance on in-house counsel in the place of outside counsel in the context of IR can be dangerous. Indeed, in-house counsel often perform both legal and business functions, and a company that does not engage outside counsel during IR efforts may face difficulty establishing that their efforts stemmed from a predominantly legal purpose. If in-house counsel is providing advice that is not strictly legal in nature, or if in-house counsel serves multiple roles (which is often the case), the risks increase. Thus, the hiring of outside counsel is a factor courts take into consideration when assessing whether attorney–client privilege (and especially the work product doctrine) applies. Once outside counsel is retained, let outside counsel direct and supervise the incident response, including the hiring of any third-party firms that may be involved in the response (e.g., forensic companies, data mining vendors, etc.). With outside counsel in charge, companies will be in a better position to argue that their IR documents and communications stemmed from a legal need.

**Pay close attention to language in existing retainer agreements and new statements of work**

During incident response, relying on forensic companies that are on retainer to provide cyber security services to the company in its ordinary course of business has proven to be dangerous from the privilege perspective. While a company may have valid reasons to use a company already on retainer (e.g., the company is already familiar with the company's systems and environment; less contract negotiation during an incident), companies and outside counsel must take caution when taking this route. Courts often take the view that companies on retainer are providing services for a primary business purpose, as opposed to a legal need. Paying attention to the language used in a statement of work specific to a particular incident is critical, especially when an existing contract is in place. Among other things, the

statement of work should: 1) clearly define the legal advice sought; 3) designate outside counsel as the one directing and supervising the investigation; and 3) make clear that all written reports and communications should flow through counsel. Within the company itself, it will also be helpful to designate any forensic investigation expenses as legal expenses, as opposed to flowing through a business function, such as IT.

For example, in litigation following the 2015 Premera Blue Cross (Premera) cyber security incident, the District of Oregon closely scrutinized the wording of retainer agreements and statements of work to discern the purpose of the investigation undertaken by a forensic incident response company.[15] The court ultimately found that the results of the investigation were not protected by the attorney–client privilege or the work product doctrine, and relied on particular wording in the agreements to reach this conclusion.

Premera hired Mandiant in October 2014 to conduct routine reviews of its data management system.[16] On 20th February, 2015, Premera hired outside counsel in anticipation of litigation following the discovery of a cyber intrusion. The next day, Premera and Mandiant entered a revised statement of work that gave Premera's outside counsel supervisory authority over Mandiant's investigation.[17] The new statement did not otherwise change Mandiant's scope of work from the October 2014 statement, however.[18]

When the plaintiffs suing Premera sought to compel the disclosure of Mandiant's report, Premera argued that the report was protected by the attorney–client privilege and the work product doctrine. The court disagreed, noting that 'the only thing that changed' with respect to Mandiant's work was that 'Mandiant was now directed to report directly to outside counsel and to label all of Mandiant's communications as "privileged", "work-product", or "at the request of counsel"'. Because Premera could not show that 'Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation' versus the previous business purpose for its work, Premera could not demonstrate a predominantly legal purpose for the investigation.[19] Premera's failure to define a clear and distinct legal purpose in Mandiant's scope of work following the incident proved fatal to Premera's privilege and work product arguments, despite the fact that outside counsel assumed supervisory authority over Mandiant following the cyber security incident. Similarly, in litigation surrounding Rutter Inc.'s (Rutter's) data breach, the court forced the company to produce an investigative report prepared by Kroll Cybersecurity, LLC (Kroll) to plaintiffs.[20] Rutter's hired outside counsel the day of the suspected incident, and outside counsel hired Kroll.[21] But while outside counsel hired Kroll, Rutter's paid Kroll directly, and Rutter's personnel regularly communicated directly with Kroll.[22] Kroll's retention agreement also stated that it would 'work alongside Rutter's IT personnel to identify and remediate potential vulnerabilities' to determine 'whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data'.[23] The court concluded that the purpose of the investigation was not to determine the proper legal response to the cyber security incident, but rather to determine if there had been a cyber security incident. Despite understanding between Rutter's and outside counsel that the investigation would be privileged, the judge was not convinced that the subsequent conduct demonstrated that intended purpose.

The foregoing cases demonstrate the importance of demonstrating to a court that legal advice was the predominate purpose, including paying close attention to the language used in contracts with forensic companies. Although not ideal from a business perspective, companies may be in a better position to argue IR-efforts are protected by using a third-party forensic company that does not have a previous relationship with the company. If the company wants to use a forensic company already familiar with the company's environment, outside counsel should carefully review existing contracts and take steps to include language in the new statement of work that clearly demonstrates how the new services differ from

what was provided for in the past. Further, the statement of work must show that outside counsel is supervising the work, interacting directly with the vendor and providing instruction and direction. In a close call on predominate purpose, these actions will make it easier for a court to find that the effort was protected by privilege.

**Protections can be waived: Take caution when distributing or relying on privileged materials**

Companies also need to be careful not to inadvertently waive the attorney–client privilege. 'As a general rule, the attorney– client privilege is waived by voluntary disclosure of private communications by an individual or corporation to third parties.' For example, if the target of a cyber incident e-mails in-house counsel about preliminary investigation results, but then subsequently forwards those results to an unrelated third party (e.g., law enforcement), the privilege over the results is likely waived.

This rule has exceptions, however. Parties may 'share privileged materials with one another to more effectively prosecute or defend their claims' where the parties' 'legal interests coincide.' But these exceptions — like the privilege itself — are complicated, and subject to often strict interpretations. Particularly applicable in the incident response, a common interest in understanding factually what happened does not mean that parties share a common legal interest in the resolution of any claims. An agreement to share investigation results or conduct a joint inquiry is not an agreement to pursue a joint legal strategy. Privileged information shared under such an arrangement is subject to waiver of the attorney–client privilege. Put simply, for any protection to survive disclosure to a third party, there must be a clearly defined joint legal purpose before the disclosure. Attempts to define a common legal purpose after the fact are rarely successful.

Less stringent rules on disclosure apply to attorney work product than attorney– client privileged communications. Unlike privileged communications, work product can be shared outside the attorney–client relationship without necessarily resulting in a waiver of the doctrine's protection. But the use of documents protected by the work product doctrine for non-litigation purposes — such as diagnosing security weaknesses or evaluating the extent of a cyber security incident for business purposes — may lead a court to conclude that the document in question was not created 'because of' pending or threatened litigation. As a practical reality, companies should avoid the disclosure of work product protected documents to persons not necessary for litigation purposes (e.g., broader incident response team, law enforcement, other employees, etc.) to avoid the risk of losing the doctrine's protections.

**Dual-track investigation**

Privilege and work product doctrine claims are often challenged based on arguments that IR reports/materials were prepared for business purposes, as opposed to for obtaining legal advice or in anticipation of litigation. Some organizations have been successful in establishing protections by setting up dual-track investigations with separate teams, where one team investigates in the ordinary course of business (a non-privileged investigation) and the other team conducts a privileged investigation aimed towards providing the organization with legal advice. When following this approach, companies should gather sufficient documentation to evidence that two separate investigations have been set up and maintain a clear demarcation of roles and workflow. Companies should also consider the consequences of relying on material they are claiming privilege or work product over for other non-legal purposes (e.g., responding to regulators, improving the IR function, general cyber security improvements). From a forensic report perspective, any information that would likely only serve a business function (e.g., general

recommendations on how to improve a company's information security program) should be omitted from privileged reports, as that may blur the lines as to the purpose of the investigation.

In *Wengui v. Clark Hill, PLC*, for example, the District Court for the District of Columbia found that Clark Hill had waived the protections of the attorney– client privilege and the work product doctrine, despite setting up clearly separated investigations for litigation and non-litigation purposes.[24] Following a cyberattack resulting in a breach of client information, Clark Hill engaged outside counsel to manage potential litigation while also mounting a separate forensic investigation to determine the extent and origins of the breach. Immediately following the breach, Clark Hill engaged outside counsel, while also hiring a separate company — eSentire — to conduct an internal investigation into the breach. The outside law company in turn hired its own forensic investigators, Duff & Phelps, to investigate the breach to develop information for future litigation. When the plaintiff moved to compel Clark Hill to produce the Duff & Phelps report, Clark Hill argued that the report was protected because it was created in anticipation of litigation. Clark Hill pointed to the separate eSentire investigation as the investigation being performed for business continuity reasons.[25]

But Clark Hill's argument was unpersuasive. The court found the Duff & Phelps report — ostensibly created purely for litigation purposes — was 'shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team"'.[26] The court found that 'the fact that the report was used for a range of non-litigation purposes reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation'.[27] Clark Hill also argued the report was protected by the attorney–client privilege, but this too was rejected: '[T]he Court concludes that Clark Hill's true objective was gleaning Duff & Phelps's expertise in cybersecurity, not in "obtaining *legal* advice *from its lawyer*".'[28]

Put simply, Clark Hill's actions did not match the stated intent of the investigation. Clark Hill, with the assistance of counsel, articulated a clear legal purpose for the Duff & Phelps investigation. But when Clark Hill relied on that report for other purposes and shared that report with people outside that purpose, Clark Hill's actions no longer aligned with the intended purpose stated at the outset of the incident response plan. When actions do not align with purposes, courts may be quick to strip protections.

**Exercise caution when documenting during incident response**

Given that courts are increasingly finding incident response efforts to be a business (and not a legal) function, IR teams must be trained to document investigation efforts carefully, as if they expect the documentation and communications to be part of litigation, or even worse, make their way into the press. Indeed, an organization is only as strong as its people — all personnel should be informed that their communications are potentially discoverable. A good rule of thumb is to educate personnel to document facts, not opinions. Personnel should also be taught to avoid any unnecessary written communications and avoid speculating on the reason for, or impact of, an incident. Communications hypothesizing about a company's fault as it relates to an incident or referring to an incident as a 'breach,' which is a legally defined term, can affect an organization's legal position and create risks during litigation and enforcement actions.

## REMEMBER, FOCUS ON THE PURPOSE AND ENSURING ACTS FOLLOW THE INTENDED PURPOSE

These recent decisions, when viewed holistically, follow a common theme. Courts, in determining the applicability of the attorney–client privilege or work product doctrine to investigatory materials, will assess

the investigation's underlying purpose and motivation. Simply having outside counsel nominally hire the forensic company is not enough. Recent cases have made it clear that establishing protections involves a highly fact-sensitive inquiry, and after-the-fact attempts to shield an investigation from opposing parties will not pass judicial scrutiny. Companies — with the assistance of counsel — must clearly delineate the purpose of an investigation at the outset of the response and outline a plan for conduct that demonstrates that purpose.

Successfully maintaining attorney–client privilege and work product doctrine protections throughout the incident response process requires careful consideration and affirmative action well before a cyber security incident is detected. There is no fixed formula to ensure the protections apply, and courts will examine the detailed factual circumstances surrounding any asserted protection. In the often chaotic aftermath of a cyber security incident, companies face a daunting proposition to manage these considerations while simultaneously responding to the incident itself. But armed with the advance knowledge of the factors courts will examine to determine whether attorney–client privilege or work product doctrine protections apply, companies can take proactive steps *before* an incident to ensure their incident response plans are positioned to maintain these critical protections throughout the life cycle of a cyber security incident response.

By proactively creating an IR plan that emphasizes the primary purpose of each action with future judicial analysis in mind, companies can place themselves in the best position to demonstrate a clear purpose for each step of the IR process — and consequently, be better prepared to ensure that the most sensitive aspects of the response to a given incident remain well protected behind the attorney–client privilege or work product doctrine.

**References**


1. See for example in *Target Corp. Customer Data Security Breach Litig.*, MDL No.14-2522 (PAM/JJK), 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015) (finding protections apply where 'Target has demonstrated ... that the work of the Data Breach Task Force was focused not on remediation of the breach, as Plaintiffs contend, but on informing Target's in-house and outside counsel about the breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company [in litigation].'); *Nat. Union Fire Ins. Co. of Pittsburg, Pa. v. Murray Sheet Metal Co., Inc.*, 967 F.2d 980, 984 (4th Cir. 1992) ('Determining the driving force behind the preparation of each requested document is therefore required in resolving a work product immunity question.').
2. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).
3. 425 U.S. 391, 403 (1976).
4. See, for example in Rutter's Data Security Breach Litig., C.A. No. 1:20-cv-382, 2021 WL 3733137, at *2-4 (M.D. Pa. July 22, 2021) (examining totality of relationship between company and outside investigator, and not just individual documents, in both work product doctrine and attorney–client privilege analysis).
5. Courts have uniformly held that any documents transmitted to an attorney for the purpose of seeking legal advice, which could have been obtained by court process directly from the client, can be obtained directly from the attorney. Upjohn, 425 U.S. at 403-04 ('This Court and the lower courts have thus uniformly held that pre-existing documents which could have been obtained by court process from the client when he was in possession may also be obtained from the attorney by similar process following transfer by the client in order to obtain more informed legal advice.').
6. United States v. Nobles, 422 U.S. 225, 238 (1975).

7. Ibid.
8. Fed. R. Civ. P. 26(b).
9. Paice, LLC v. Hyundai Motor Co., 302 F.R.D. 128, 133 (D. Md. 2014) ('Materials prepared in the ordinary course of business, pursuant to regulatory requirements, or for other non-litigation purposes are not prepared in anticipation of litigation.').
10. In Grand Jury Subpoena, 220 F.R.D. 130, 147 (D. Mass. 2004) ('[A]nticipation requires something more than a mere remote possibility of litigation.').
11. In Grand Jury Proceedings, No. M-11-189, 2001 WL 1167497, at *17-18 (S.D.N.Y. Oct. 3, 2001) (government subpoena gives rise to reasonable anticipation of litigation); Cal. Earthquake Auth.
12. v. Metro W. Sec., LLC, 285 F.R.D. 585, 590 (E.D. Cal. 2012) (request for mediation creates threat of litigation); Kan. City S. Ry. v. Nichols Constr. Co., C.A. No. 05-1182, 2007 WL 2127820, at *5 (E.D. La. July 25, 2007) (particularly severe nature of incident creates reasonable anticipation of litigation).
13. See Johnson v. Air Liquide Large Indus. U.S. L.P., Case No. 2:18-CV-259, 2019 WL 4256962, at *5 (E.D. Tex. Sept. 9, 2019) (finding intent to preserve evidence relevant to determining whether reasonable anticipation of litigation existed for work product protection).
14. United States v. Aldman, 134 F.3d 1194, 1202 (2d Cir. 1998) ('[T]he "because of" formulation that we adopt here withholds protection from documents... that would have been created in essentially similar form irrespective of the litigation.').
15. Paice, 302 F.R.D. at 133.
16. In re Premera Blue Cross Customer Data Security Breach Litig., 296 F.Supp.3d 1230 (D. Or. 2017).
17. Ibid., at 1245.
18. Ibid., at 1245.
19. Ibid., at 1245.
20. Ibid., at 1245.
21. In re Rutter's Data Security Breach Litig., 2021 WL 3733137, at *1.
22. Ibid.
23. Ibid.
24. Ibid., at *2-3.
25. 338 F.R.D. 7, 9 (D.D.C. 2021).
26. Ibid. at 11.
27. Ibid.
28. Ibid.
29. Ibid. at 13 (citations omitted) (emphasis in original).

**Co-author, "The Do's and Don'ts of Cybersecurity Forensic Investigations," *Law360*, August 26, 2022.**

According to the Verizon Wireless 2022 Data Breach Investigations Report, there are four prominent paths that threat actors use to gain unauthorized access into an organization's network:

1. Stolen or compromised credentials;
2. Phishing;
3. Exploiting vulnerabilities; and
4. Botnets.

Threat actors have exploited these four attack vectors to unlawfully access thousands of businesses, including those that are security-forward, forcing those business to respond to often costly cybersecurity incidents.

For example, according to IBM's 2022 Cost of Data Breach Report, breaches caused by stolen or compromised credentials had an average cost of $4.5 million. These costs include both the direct and indirect expenses.

Direct expenses include "engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services." Indirect costs include in-house investigations and communications.

Luckily for businesses, not all cybersecurity incidents require the same response or lead to the same costly outcomes. Not every potential phishing scam or exploited vulnerability will trigger the need to conduct a forensic investigation or to prepare a forensic report.

For many organizations, there may be dozens, hundreds or even thousands of security alerts triggered daily.

So when do businesses need to retain forensic experts to assist with potential or actual security incidents? As with many legal questions, the answer is that it depends.

**What Is a Forensic Investigation?**

A forensic investigation is an investigation performed by an independent third party, often under the cloak of legal privilege. The investigation's purpose is to understand the nature, size and scope of the incident and to ensure that it is contained.

Consistent with its purpose, forensic investigators usually look to answer:

- Whether the network has been accessed by a threat actor;
- How the threat actor gained access to the network, i.e., root cause;
- What the threat actor did while in the network, e.g., lateral movement or access/exfiltration of data; and
- If the incident has been contained or eradicated.

After the investigation, investigators usually issue a forensic report — or a functionally equivalent document — detailing the nature of the investigation and their findings.

**Why Is a Forensic Investigation Needed?**

From a cybersecurity perspective, a forensic investigation may be needed to ensure the incident is contained and the threat fully eradicated.

Unfortunately, organizations often overlook forensics when an incident causes significant business interruption, e.g., in a ransomware attack, or when funds have been lost, e.g., in a wire transfer scam.

The focus, instead, is often on the recovery process, which may include restoring systems from clean backups, attempting to recoup lost funds, rebuilding systems from scratch, etc. Businesses must be careful, however, as returning to normal operations when the incident has not been contained may only lead to further damage.

For example, in a ransomware attack, restoring systems from clean backups when the threat actor still has a foothold in the system may prove fruitless if the threat actor can later encrypt the clean backups or execute a different exploit — e.g., exfiltration of trade secrets or sensitive consumer data.

Likewise, in a wire transfer scam, focusing only on the recovery of lost funds would be detrimental if a threat actor is still able to monitor the organization's emails, which may allow for subsequent attacks.

Conducting a forensic investigation is therefore critical to ensure that the incident is contained and eradicated and there are no hidden exploits or back doors into the network left behind.

So does every incident require a forensic investigation? No, of course not. Whether a forensic investigation is needed is likely a matter of judgment, and may require engaging different teams — e.g., information security, legal, information technology, product, etc. — to assist with the decision-making process.

This is one reason why cyberinsurance is beneficial as it provides businesses with access to readily available experts — such as outside counsel and forensic firms — who have substantial experience with these types of matters and can provide guidance in connection with the same.

**Why Can the Business Not Conduct the Investigation Itself?**

Businesses may shy away from third-party forensic investigations for one simple reason — they cost money. This is especially true when the business believes, often in good faith, that its security team can perform the same investigation without incurring any additional costs.

While there may be situations when engaging a third-party forensic firm is not needed, businesses must be mindful of the legal implications of doing so.

Typically, third-party forensic firms are retained by outside counsel on behalf of the victim-business for the purpose of seeking or obtaining legal advice and/or in anticipation of litigation. This, in turn, allows businesses to claim privilege and work-product protection over the investigation and related communications.

While recent judicial decisions have reaffirmed that establishing these protections involves a highly fact-sensitive inquiry, businesses may have a difficult time arguing that protections apply to investigations conducted internally, which are likely to be viewed as serving a business — and not a legal — purpose.[1]

Because privilege is meant to permit candid and open communications without fear of them being used against the company, conducting a privileged forensic investigation that is intended, in part, to stop a criminal from further harming the company is likely in every organization's best interest.

Businesses may also want to engage a third-party firm to perform the investigation for optics. Indeed, being able to relay to regulators and affected individuals that a specialized third-party forensic firm was engaged to determine the nature and scope of the incident may not only be helpful when communicating

about the incident but may also be expected — e.g., when reporting a data security incident to regulators, several of them require businesses to indicate whether a forensic investigation was performed.

Failing to do so may lead to further questions about the investigation itself and whether it was thorough and complete.

Lastly, engaging a third-party firm to perform the investigation may remove the appearance of bias. While certain in-house security professionals may actually be in the best position to investigate the cause and scope of a cybersecurity incident given their familiarity with the network, this could create obstacles — from an optics perspective — that could otherwise be avoided if a third party is used.

**Do's and Don'ts of Forensic Reporting**

Investigators usually issue a forensic report at the end of the investigation detailing the nature of their investigation and findings. While these reports should be privileged when the relationship is set up properly through counsel, a good rule of thumb when it comes to forensic reporting is to assume that it will be part of litigation later on.

To this end, businesses, law firms and even forensic firms must take caution when drafting forensic reports.

Below are a few steps all involved parties can take to minimize the chance of creating bad documents.

**Clearly Describe the Objectives of the Investigation**

Often, businesses may engage a third-party forensic firm to conduct only certain aspects of the investigation. Thus, it is important for forensic reports to clearly describe the objectives of the investigation — i.e., what was the forensic firm tasked with — and the results of the investigation.

If a report does not discuss certain aspects of an investigation, and the investigation objectives are not delineated, one may assume that the report, and consequently the investigation, were incomplete.

**Is a Forensic Report Even Needed?**

Before tasking a forensic firm with drafting a forensic report, it is important for counsel to advise the risks and benefits of obtaining a report given the affected businesses' intended use of the report.

If the business wants a report to share the investigation findings with customers and clients, for example, then a forensic report may not be useful.

**Forensic Reports Are Nonfiction Writings**

Forensic reports should be purely factual. There is no room for imagination, opinions or speculations.

Rather, everything documented in a forensic report should be based on facts and supported by forensic findings.

**Put Conclusions Upfront**

This is a forensic report — there is no need for a plot twist.

Let the reader know upfront, perhaps in an executive summary, whether there was any unauthorized access or exfiltration of data or files. This point is critical as it determines whether the incident qualifies as a data breach under applicable laws.

No unauthorized access or exfiltration of data? State that clearly upfront as well.

**Avoid Arbitrary Gradings, Scales or Severity Scores**

Everyone involved in the drafting process needs to be mindful that forensic reports are often used against companies during litigation and regulatory investigations.

Assigning arbitrary grading scales or severity scores to the incident, or even components of the incident, are not likely to be useful to the business and will likely be used against the business should the document become discoverable.

**Omit General Security Recommendations**

While it may be tempting to include security recommendations in a forensic report, recent case law suggests that doing so may hurt the business's position that the document was created for legal purposes.

Thus, it is recommended to omit security recommendations from the report altogether, and have that discussion verbally, if needed.

For this same reasons, forensic firms should also avoid using forensic reports as a means to sell other products or services.

**Mark it Privileged and Confidential**

If the forensic report is intended to be protected, be sure to mark it as such.

While failing to do so will not likely compromise the protections, it will likely create unnecessary obstacles that could have been avoided if the proper markings were included.

## Co-author, "Four Strategies for Drafting Effective Consumer Breach Notices," *Law360*, September 30, 2022.

It is 2022, which means you've received your fair share of consumer breach notification letters.

At first glance, all the letters seem to look and say the same. Usually separated into five sections — we can thank California for that — the notices explain what happened, what personal information was involved, what the business is doing in response to the incident, what consumers can do to protect themselves and who the consumer can contact for additional information.

While there are formulaic requirements for consumer breach notifications, businesses responding to data security incidents should not treat their notification letters as a copy and paste exercise.

Businesses should instead approach these notices like every other step in the incident response process — as a tool intended to inform consumers while managing the business impact and legal risk.

Effective communication during the incident response process can have a lasting effect on the company, and often these communications start with the breach notice.

So what should businesses be considering when drafting these notices? Below are our top four strategies for effective consumer breach notification letters.

**1. Know your audience and what is on their mind.**

When drafting notices, it is important to know and understand your audience.

You should consider what questions the notification letter recipients will have when reading the notice in order to resolve those questions through the notice to minimize any follow-up or escalations. In the context of breach notifications, the audience is consumers and regulators.

Consumers are interested in learning how the incident relates to them personally, while regulators are interested in the business's response to the incident, including notification timing and information security improvements, and knowing whether the business is being transparent and direct about the incident while providing consumers with enough information and resources to protect themselves.

From a consumer perspective, questions that often arise include:

- Why do you have — or still have — my information?
- What specific information of mine was involved?
- Am I the victim of identity theft or other crime?
- What do I need to do?
- Can you delete my information?

From a regulator perspective, the focus is often on the following:

- Why did it take so long to provide notice?
- What security safeguards were in place before the incident?
- What changes has the business made to prevent the incident from recurring?

While the answers to some of the questions above are often included in breach notices at a high level, businesses should consider whether it is prudent to answer these questions more fulsomely, both in the breach notice and in prepared communication plans, e.g., FAQs.

For example, businesses should consider disclosing facts that would help consumers reach the conclusion that simply receiving a breach notification letter does not mean that the consumer is, or ever will be, the victim of identity theft.

For example, did the business conduct any dark web monitoring to confirm that exfiltrated data was not leaked? Did the business pay a ransom and receive assurance from the threat actor that data will not be further disclosed? Was there no evidence of data exfiltration?

Assuming these steps were taken, disclosing them in a breach notice may go a long way in addressing the questions on most consumers' minds. These statements, however, should not be drafted to steer the consumer away from taking certain precautionary steps, such as signing up for credit monitoring.

It is easy to make statements quelling consumers' concerns that at the same time may trigger regulatory scrutiny. It is, therefore, important to strike an appropriate balance.

Ultimately, consumers should always be encouraged to take steps to protect their personal information, and it should be up to consumers to decide whether there is no risk based on the facts.

Likewise, a few sentences explaining the timeline from the discovery of the incident to the date of notifications may alleviate regulators' timing concerns if this information is provided upfront.

For example, if data mining was a step taken as part of the response, explaining that a third-party vendor was hired to assist with determining the affected population may provide regulators with comfort as it is expected that this process will take time, and the business is taking the requisite steps to determine the nature and scope of the population requiring notification.

Businesses may also benefit from a statement indicating that at the time of discovery there was just not enough information to provide notifications. Time is needed to conduct the investigation, to determine whether notification is required, and, if so, to whom.

When appropriate, businesses may also want to consider the benefit of talking to regulators early and often, rather than waiting for the dreaded follow-up.

**2. Consider the business, products and services at issue.**

One question that consumers always ask is: "Why do you have — or still have — my information?"

This question highlights the need for businesses to begin breach notification letters with an explanation about the business and the products and services it provides.

For example, if you are a business that consumers are not likely to remember conducting any transactions with — e.g., a third-party service provider that has agreed to provide notice on behalf of another organization — explaining your relationship with the consumer, and why you have the consumer's information, is critical.

Having a good privacy policy businesses can point back to that explains what data is collected and for what purposes would help.

Even for businesses that have a direct relationship, consider the personal information involved in the incident and explain the context around why the personal information was properly collected. For example, if you're a retailer, why do you have a consumer's passport information? Perhaps it was collected in the context of a return and collected for identification purposes.

Explaining why the affected business has the information at issue reduces the number of individuals contacting the call center, and may provide a sense of relief and trust to the letter recipient.

This is also beneficial from a regulatory perspective and it likely will result in a reduced number of consumers contacting their attorney general's office to complain.

**3. Exercise caution when making statements about the organization's information security posture.**

The California Consumer Privacy Act, which soon will be significantly modified by the California Privacy Rights Act, allows consumers to bring an action for statutory damages in the event of a data breach due to a business's failure to implement reasonable security procedures.

However, before bringing an action, the consumer must provide the business with 30 days' written notice identifying the specific violation. If the business cures the noticed violation and provides the consumer a written statement indicating such, statutory damages are not available.

What qualifies as a cure remains unclear, but businesses should give careful thought to their breach notice as well as the written response.

On one hand, if a business believes that reasonable security procedures are intact, the business's breach notice, written response and actions should communicate this message consistently.

Statements concerning the health of the business's security environment in a breach notice — e.g., "we apologize that our security procedures did not meet your expectations" — or any changes to existing security procedures in the event of a breach will be a double-edged sword, so businesses should take caution.

On the other hand, if a business believes that heightened data security procedures are warranted, it would be wise to frame these steps — to the extent factually accurate — as steps the business is taking as part of its ongoing assessment of its information security program.

In other words, the changes should not be worded to suggest that certain safeguards or controls were previously lacking. Indeed, cybersecurity is a rapidly moving target, and thus consumers and regulators should expect to see such changes, especially after a data security incident.

**4. Prioritize user-friendliness and tone.**

If you have been tracking what's been happening in California concerning the CCPA and related enforcement efforts, you may know that there is increased attention on the manner in which information is conveyed to consumers.

The use of headers, bullets and bolded font especially with respect to the "what you can do" section, may help achieve this goal.

Businesses should also consider the demographics of their audience, including their ages and locale. For less technically savvy audiences, avoiding unnecessary legal or technical jargon is important to ensure the message does not get lost in translation,

Businesses should also involve the internal communications team in the drafting process to ensure that the tone of the notification matches the business's day-to-day messaging style. A breach notice that takes a sharp turn from standard messaging may trigger unnecessary fear or come off as disingenuous.

Public relations firms may be especially helpful in this context as they can provide honest feedback, from an outsider's perspective, how certain messaging may be received and what narratives may not work for the organization.

The consumer notification process should not be treated as a check-the-box exercise. Notification is a step in the incident response process businesses would be wise to use to minimize the incident's impact on the organization.

## Co-author, "SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on their Security and Disclosure Plans," *Troutman Pepper*, July 31, 2023.

On July 26, the Securities and Exchange Commission (SEC) adopted, by a 3-2 margin, a final rule to require more immediate disclosure of material cybersecurity incidents by public companies. In addition, the final rule requires annual disclosure of material information regarding a public company's cybersecurity risk management strategy and cybersecurity governance.

In approving the final rule, SEC Chairman Gary Gensler stated that the final rule will provide investors with more consistent, comparable, and decision-useful tools for analyzing disclosures about cybersecurity incidents. The reality is that the final rule requires public companies to make difficult real-time decisions about whether a cybersecurity incident requires disclosure, all while in the middle of responding to and addressing the actual incident. When a cybersecurity incident inescapably happens, the right information must be reported up the chain to those making disclosure decisions. Public companies should consider identifying gaps in reporting structures and increasing collaboration among security teams and legal counsel.

**Compliance Deadlines**

The final rule becomes effective 30 days after publication in the *Federal Register*. The new disclosures will need to be incorporated into Form 10-K and Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023. The new disclosures will need to be incorporated into Form 8-K and Form 6-K beginning December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosures. All public companies must tag disclosures required under the final rule with iXBRL beginning one year after initial compliance with the related disclosure requirement.

**Material Cybersecurity Incidents Must be Disclosed on Current Reports on Form 8-K**

The final rule adds a new disclosure requirement to Item 1.05 of Form 8-K that will require public companies to disclose any "cybersecurity incident"[1] determined to be material. The Form 8-K must be filed within four business days of a public company's materiality determination. That is, a public company is not required to make the cybersecurity disclosures within four business days of the discovery of a cybersecurity incident, but within four business days of the date that the company determines that the

cybersecurity incident is material. In assessing materiality, the final rule adopted the long-accepted definition of "materiality" from *TSC Industries, Inc. v. Northway, Inc.* 426 U.S. 438 (1976), *i.e.*, something is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available." A company must make this determination without "unreasonable delay after discovery of the incident." The Item 1.05 disclosure must describe (1) the material aspects of the cybersecurity incident, including the nature, scope, and timing of the incident; and (2) the material impact, or reasonably likely material impact, of the cybersecurity incident on the company, including its impact on its financial condition and results of operations.

The new Form 8-K disclosure requirement encompasses disclosure of material incidents that occur on a public company's third-party systems (such as cloud-hosted systems). While acknowledging that public companies will have less visibility into third-party systems, the SEC stressed that public companies should make their disclosure based on the information available to them. The final rule generally does not require public companies to conduct additional inquiries outside of their regular channels of communication with third-party service providers.

In response to public comments, the SEC made several significant changes from the proposed rules (described here). To balance the most common criticisms of the proposed Item 1.05 requirements reported during the comment process concerning the scope and timing of the disclosure, the final rule narrowed the information required to be disclosed. As adopted, the final rule does not require disclosure of: (1) the incident's remediation status; and (2) information about the company's planned response to the incident, its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail that would impede the company's response. As such, the final rule attempts to focus disclosures on the material impact of a cybersecurity incident rather than requiring extensive details about the incident itself, which critics argued could be misused by malicious actors. The SEC noted, however, that it was not persuaded that it should forgo requiring disclosure of the existence of an incident while it is ongoing. As to concerns with timing of the disclosure, the SEC stated that by reducing required disclosures to information "focused on an incident's basic identifying details and its material impact or reasonably likely material impact" public companies should have all the information necessary to make the disclosure.

Additionally, the final rule provides for a limited delay of the Form 8-K disclosure for cybersecurity events that could pose a "substantial risk to national security or public safety." However, a company's ability to earn this relief requires the intervention of the U.S. attorney general. If a public company persuades the attorney general that the required disclosure would pose a substantial risk to national security or public safety, disclosure may be delayed for 30 days following the date when the disclosure was otherwise required to be provided. The attorney general must notify the SEC of such determination in writing. After the initial delay notification period, the attorney general may recommend, subject to the SEC's discretion, additional delays of up to 60 days if disclosure would still pose a substantial risk to national security or public safety. Beyond that, additional requests for delay may be considered through exemptive orders. To facilitate such communications, the SEC noted that it consulted with the Department of Justice to establish an interagency communication process – but details on how this process would work were absent in the final rule.

Finally, as proposed, the late disclosure of an Item 1.05 Form 8-K would not result in a loss of S-3 eligibility.

***Updates with a Form 8-K Amendment***

In a significant change from the proposed rule, the SEC did not require updates to cybersecurity incidents previously reported under Item 1.05 of Form 8-K be reported in periodic reports. Instead, public companies must make such updates through an amended Item 1.05 disclosure on Form 8-K. The instructions to Item 1.05 of Form 8-K will require a public company to identify any information required by Item 1.05 that was not determinable or was unavailable at the time of the required filing. When such information becomes available, the company must file an amended Form 8-K within four business days. The SEC specifically noted that the final rule does not require an amended Form 8-K for all new information, but only for that information required by Item 1.05 of Form 8-K that was unavailable at the time the initial Form 8-K was required. The final rule does not separately create or otherwise affect a company's duty to update its prior statements.

***Practical Guidance***

Security teams and legal counsel should collaborate to determine whether an incident is material. This will challenge companies to balance timely disclosure with accurate disclosure. No incidents are equal in size and nature; what may seem like a material incident can later be deemed immaterial and vice versa. Companies should ensure incident response plans account for consistent communication flows among key stakeholders. It does not matter how robust a security response plan is if the information does not make its way to those making disclosure decisions or if it is not reported in time.

Whether an incident is material also does not solely depend on a financial threshold. A public company should consider harm to such company's reputation, customer or vendor relationships, competitiveness, or the possibility of litigation or a regulatory investigation, from state, federal, and non-U.S. authorities when determining whether disclosure is required.

Once a company determines a cybersecurity event has occurred, it must make a materiality determination without "unreasonable delay." While public companies should generally be experienced in applying the *TSC v. Northway* materiality standard, many companies may not be comfortable applying these standards to a cybersecurity incident.

A company should not delay filing a Form 8-K once the cybersecurity event is deemed material even if material information is "undetermined or unavailable" at the time of the initial Form 8-K filing. The instructions to Item 1.05 of Form 8-K specifically envision this scenario and permit amendments to the Form 8-K to be filed as such material information becomes known. A company should also correct any prior disclosures made under Item 1.05 of Form 8-K that such company later determines were untrue at the time they were made or become materially inaccurate after they were made.

Public companies should also consider whether a series of cybersecurity incidents, taken as a whole, cross the materiality threshold, rather than failing to disclose the incidents because each incident was determined to be immaterial.

**Annual Disclosure Obligations**

The final rule also amends Form 10-K and adds new Item 106 to Regulation S-K to require updated cybersecurity disclosure in Form 10-Ks concerning how public companies manage and govern for cybersecurity risks.

The amendment to Form 10-K adds new Item 1C. Cybersecurity to Part I of Form 10-K, which will require the disclosures mandated by Item 106 of Regulation S-K. New Regulation S-K Item 106(b) will require public companies to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. It will also require a public company to describe whether any risks from cybersecurity incidents have, or are reasonably likely to, materially affect such company, including its business strategy, results of operations, or financial condition. The final rule limits the level of detail required to be disclosed regarding a public company's internal processes to information that is material to investors in order address concerns that requiring additional detail could increase a public company's vulnerability to cyberattack. In addition to adding a materiality qualifier to the required disclosures, the final rule also reduces the amount of granular disclosure required by the proposed rules.

New Regulation S-K Item 106(c) will require public companies to describe the board's oversight of risk from cybersecurity threats, identify a board committee or subcommittee responsible for such oversight, if any, and describe the processes by which the board or such committee or subcommittee is informed about such risks. Item 106(c) will also require disclosures describing management's role in assessing and managing material risks from cybersecurity threats, including identifying which management positions and committees are involved, the processes undertaken, and how management reports cybersecurity risks to the board. Similar to its approach to Item 106(b), the SEC reduced the disclosures required from those in proposed Item 106(c), added materiality qualifiers, and adopted a relatively less granular approach.

The final rule does not require public companies to disclose (as proposed): (1) whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight; or (2) the frequency of discussions on cybersecurity. The final rule also did not adopt the proposal to require disclosure about the cybersecurity expertise, if any, of a public company's board members.

***Practical Guidance***

Item 106 – and the final rule as a whole – make it clear that cybersecurity threats are no longer just an IT problem. Boards will be required to oversee the collaborative efforts to protect against and respond to cyber threats. What has traditionally been a reactive process will slowly shift to a proactive collaboration among various key stakeholders.

Security teams and legal counsel will again need to work together to draft the disclosure to ensure the information is accurate, relevant, and necessary. Companies responding to cybersecurity incidents face the difficult task of managing incident response efforts while maintaining attorney-client privilege protections. As with forensic reports, disclosures should be factual and avoid speculations or opinions. While a company may want to minimize the impact of the incident, companies that fail to be forthcoming with information can face probes and potential penalties from the SEC for misleading investors. This means companies should create and/or tailor incident response plans to be effective in providing guidance on how to identify and respond to red flags. These response plans should be consistently tested and reviewed to keep up with the evolving threats. Again, these disclosures will require collaboration from multiple key stakeholders.

Public companies are not required to disclose formally adopted cybersecurity policies and procedures, which could lead to the disclosure of operational details that could be weaponized by cyber criminals. Rather, a public company can still comply with the newly adopted Items 106(b) and (c) of Regulation S-K by focusing disclosures generally on its risk assessment and putting a governance program in place and

discussing how such programs have evolved given changes in the company's material cybersecurity risks.

Public companies should consider the following when describing management's role in assessing and managing material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of those individuals in enough detail to fully describe the nature of the expertise;
- How such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board or a committee or subcommittee of the board.
- Additionally, although the frequency of discussion on cybersecurity is not an express requirement under Item 106(c)(1), a public company should consider whether a discussion of frequency should be included in its description of how the board or relevant committee is informed about cybersecurity risks.

**Application to Foreign Private Issuers**

The final rule is applicable to foreign private issuers (FPIs) and modifies Forms 20-F and 6-K to require disclosures concerning material cybersecurity incidents similar to those required by public companies using domestic filing forms. The final rule amends Part II of Form 20-F by adding Item 16K, which has language identical to that in new Regulation S-K Item 106. Form 6-K was modified by amending General Instruction B to include material cybersecurity incidents among the items triggering a Form 6-K filing.

The SEC, however, declined to require Canadian FPIs utilizing the Multi-Jurisdiction Disclosure System (MJDS) to make the annual disclosure requirements enumerated in Regulation S-K Item 106 (and added to Form 20-F) when filing annual reports on Form 40-F. Given that such filers are already subject to the Canadian Securities Administrator's 2017 guidance on the disclosure of cybersecurity incidents and that the MJDS generally permits such filers to use Canadian disclosure standards and documents, the SEC did not find a reason to adopt prescriptive cybersecurity disclosure requirements for 40-F filers.

**Structured Data Requirements**

The SEC adopted the Structured Data Requirements as proposed, which requires public companies to tag the information specified by new Item 1.05 of Form 8-K and new Items 106(b) and (c) of Regulation S-K with Inline XBRL (iXBRL) in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

**Criticism of the Rule**

In dissenting from the final rule, Commissioner Hester Peirce delivered an excoriating critique listing a series of question and open interpretative issues that the final rule does not address. Commissioner Mark Uyeda also dissented from the adoption of the final rule and criticized it as elevating cybersecurity disclosures above other risks and issues that may be more material to investors.

Peirce raised concerns with the SEC's expansive view of its authority as expressed in the final rule, warning that it "reads like a test run for future overly prescriptive, overly costly disclosure rules covering a never-ending list of hot topics." In her view, the expansive view of the SEC's authority manifests itself in three ways throughout the final rule. First, the rejection of financial materiality as the touchstone for disclosures, causing the granular disclosures the final rule requires to "seem designed to better meet the needs of would-be hackers" rather than investors. Second, the required governance disclosures read like a compliance checklist that would have the SEC managing public companies' cybersecurity and will "drive companies to spend resources on compliance with our rules and conformity with other companies' disclosed practices, instead of on combatting cyber threats as they see fit." Finally, Peirce was concerned with the SEC's refusal to consider other cybersecurity rules and a failure to "defer to other government agencies with overarching mandates to protect national security, public safety, and critical infrastructure." In a similar vein, she noted that getting the necessary approval from the U.S. attorney general — within four days — to use the national security or public safety exemption "will be quite a feat."

Additionally, Peirce worried that the final rule's prescriptive approach will impose considerable costs on investors, arguing that a more flexible, principles-based approach would be a better way to protect investors. Her views on these costs can also be broken down into three categories. First are the direct compliance costs that public companies will face in complying with the final rule — a matter the final rule admits it is generally unable to quantify. In this compliant, she was joined by Uyeda, who found the SEC's determination that the final rule was not a "major rule" under the Small Business Regulatory Enforcement Act, completely uncredible, as the comments suggested that compliance costs could be well in excess of $100 million. Second, Peirce warned that the disclosures will aid cyber criminals by handing them a roadmap of which companies to target and how to attack. And third, she worried that disclosures might "mislead otherwise uninformed investors without first-hand knowledge of cyber attacking" while "the fast timeline for disclosing cyber incidents could lead to disclosures that are tentative and unclear, resulting in false positives and mispricing in the market."

In closing her dissent, Peirce raised several questions that registrants will have to wrestle with as they begin to prepare the disclosures required under the final rule, including:

- Whether public companies will have to develop new systems to track immaterial cybersecurity incidents given that the definition of "cybersecurity incident" includes "an unauthorized occurrence, or a series of related unauthorized occurrences."
- Given that "related" is not defined, how will a company determine whether to aggregate occurrences for purposes of determining whether to file a Form 8-K?
- "Cybersecurity incident" is defined to include anything that "jeopardizes" information systems. Under this definition, a cybersecurity incident could occur whenever information is merely at risk even if not actually stolen. Won't companies have difficulty tracking cybersecurity incidents, so broadly defined?
- Will public companies become less nimble in updating their cyber policies and procedures because they would have to simultaneously change their regulatory filings?

Uyeda also criticized the final rule for elevating cybersecurity disclosures above other risks and issues that may be more material to investors. Uyeda worried that the final rule, by neglecting financial materiality standards, advances an overly prescriptive standard without a meaningful discussion as to why there should be an increased focus on cybersecurity risks, as compared to other risks that potentially could have a greater material impact on a public company. He also lamented that the final rule "breaks

new ground" in mandating real-time, forward-looking disclosure by requiring companies to assess a cybersecurity incident's material impact while the incident is ongoing.

**Five Things Companies Subject to the new SEC Cyber Requirements Have to Do Now (or at least before December 2023):**

1. **Update Incident Response Plans** to Add New SEC Disclosure Process, including definitions and timing triggering notification that balance transparency, accuracy and maintaining level privilege.
2. **Develop Template Annual Reporting (Form 10-K and new Item 1C) and Periodic Reporting (8-K) Templates** just like companies develop template regulatory, HR, consumer and B2B breach notification notices.
3. **Have Legal/General Counsels and CISOs Collaborate**, including around identifying and conducting assessment around a cybersecurity framework for the organization and corresponding key controls (e.g., CIS-18, NIST Cybersecurity Framework and ISO 27001)
4. **Global Companies Identify Exceptions for Foreign Public Issues Covered under Local Country Laws**, including Canadian Foreign Public Issuers utilizing the Multi-Jurisdiction Disclosure System (MJDS) utilizing Form 20-F when filing annual reports on Form 40-F.
5. **Develop Data Classification Policies to Help Support Calculation of Materiality** including the Business Criticality and Regulatory Impact) of the Breach of Theft of Business Crown Jewels.

Contact your Troutman Pepper attorney or any of the authors of this article if you need more information or assistance in compliance with the final rule.

# Our Team


## Ronald I. Raether Jr.

Partner
Orange County

ron.raether@troutman.com
D 949.622.2722


Ron is known as the interpreter between businesses and information technology. This experience allows him to bring a fresh and creative perspective to data compliance issues with the knowledge and historical perspective of an industry veteran.

**Areas of Focus:**

- Privacy + Cyber
- Financial Services Litigation
- Class Action
- Consumer Financial Services

Ron leads the Privacy + Cyber team at the firm, and is a partner in the Consumer Financial Services Practice Group. Ron has assisted companies in navigating federal and state privacy laws for more than 20 years. His understanding of technology led him to be involved in legal issues that cross normal law firm boundaries, including experience with data security, data privacy, patent, antitrust, and licensing and contracts.

His involvement in seminal data compliance and data use cases has helped define current standards in several areas of the law. He assisted one of the first companies required to provide notice of a data breach and has since successfully defended companies in more than 200 class actions. Even as regulators fight to broaden their authority and extend the boundaries of existing statutory schemes like the FCRA to cover data analytics and usage, Ron has adapted his practice to address this unique and shifting business/technology concern.

Ron has represented companies in hundreds of individual FCRA cases involving CRAs, resellers, furnishers, users, and public record vendors and has developed a reputation for assisting companies not traditionally viewed as subject to the FCRA. Ron also has litigated cases involving the DPPA, VPPA, TCPA, and other federal and state statutory schemes which regulate the use or security of data. Most recently, Ron has counseled clients on operationalizing the California Consumer Privacy Act of 2018 (CCPA). By relying on his knowledge of and experience with other federal and state privacy laws, Ron has enabled companies

to navigate around the ambiguities of the CCPA and make compliance decisions that are informed, well-reasoned, and still in line with their business goals.

Ron has used this broad legal experience with privacy issues and his understanding of technology to represent clients in a broad range of matters including data aggregation and analytics, mobile applications, payment technologies, de-identification/anonymization, correlation of data from multiple connected devices, "connected-things (IoT)," and electronic crash- and consumer-reporting systems.

Ron also advises on pre- and post-incident compliance concerns ranging from privacy policy preparation to development of incident response plans and workflows, addressing post-incident aftermath, and responding to regulatory inquiries. Balancing privacy, cyber security, and business functionality, Ron's approach to data governance is uniquely designed with the industry in mind as it adapts to the ever-evolving technological and legal landscape.

As a thought leader on these issues, Ron regularly speaks nationally and publishes frequently on cutting-edge compliance developments. Ron is also a Certified Information Privacy Professional.

*Representative matters may include engagements before joining Troutman Pepper.*

## Related Practices and Industries

- Privacy + Cyber
- Financial Services Litigation
- Class Action
- Consumer Financial Services
- Advanced Technology: Leading-Edge Issues
- Data + Privacy
- Data Centers
- Consumer Law Compliance
- Consumer Reporting Agencies + Background Screening
- Energy Policy + Legislation
- Fair Credit Reporting Act (FCRA)
- Fair Debt Collection Practices Act (FDCPA)
- Litigation + Trial
- Payments + Financial Technology
- Mortgage Lending + Servicing
- Incidents + Investigations
- Telephone Consumer Protection Act (TCPA)

## Speaking Engagements

- Panelist, "Financial Privacy, Data and Security," American Bar Institute's 13th Annual National Institute on Consumer Financial Services Basics, October 19, 2023.

- Speaker, "Testing Screening Operations for Potential Unintended Discrimination," Professional Background Screeners Association, September 12, 2022.
- Speaker, "Understanding the Role of Cybersecurity Expert Witness," RSA Conference, June 7, 2022.
- Speaker, "The War on Tenant Screening: How Regulatory and Legislative Changes in Washington Are Impacting the Industry," PBSA, April 11, 2022.
- Moderator, "Attorney Client Privilege in Incident Response," NetDiligence's Cyber Risk Summit, February 1, 2022.
- Panelist, "Financial Privacy and Data Security," American Bar Association's Consumer Financial Services Basics Virtual Conference, October 21, 2021.
- Speaker, "Rise of the Machines: Using AI and Other Data Analytics to Improve Compliance and Deliver Better Products," PBSA, September 13, 2021.
- Speaker, "How 2020 Vision Has Blurred Attorney Client Privilege in Incident Response," RSA Conference, May 17, 2021.
- Speaker, "Three Reasons Why 2021 Is a Good Year to Review Your Privacy Compliance Program," Troutman Pepper, March 31, 2021.
- Moderator, "Strategies to Prepare for Six Potential Target Areas of CCPA Enforcement by the CA Attorney General," Troutman Pepper Webinar, August 19, 2020.
- Presenter, "The Nuts and Bolts of CCPA 2.0," Troutman Sanders and Pepper Hamilton Webinar, June 10, 2020.
- Presenter, "COVID-19: CCPA and Regulatory and Governmental Litigation Update," Troutman Sanders Webinar, May 7, 2020.
- Speaker, "COVID-19 in the Screening Industry Q&A Part 1," PBSA Webinar, April 3, 2020.
- Speaker, "Quick Answers to Critical COVID-19 Compliance Questions for Financial Services Companies," Troutman Sanders Webinar, March 31, 2020.
- Speaker, "Incident Response Plans: Global Compliance Mandates and Obligations," ISMG Fraud & Breach Summit, December 3, 2019.
- Speaker, "Getting Your Ducks in a Row for the California Consumer Privacy Act," Receivables Managements Association International Webinar, October 23, 2019.
- Panelist, "Cyber Resiliency Beyond Data Protection," NetDiligence Cyber Risk Summit, Santa Monica, CA, October 15-17, 2019.
- Speaker, "Critical Litigation Developments Affecting the Screening Industry: 2018 – 2019 in Review," 2019 National Association of Professional Background Screeners Annual Conference, San Antonio, TX, September 8-10, 2019.
- Speaker, "Changes in California Relating to the California Investigative Consumer Reporting Agencies Act (ICRAA) - What You Need to Know and How to Comply," Troutman Sanders Webinar, April 24, 2019.
- Speaker, "Incident Response Plans: Global Compliance Mandates and Obligations," iSMG Legal & Compliance Summit, New York, NY, November 15, 2018.
- Speaker, "Cloudy With a Chance of Legal Action: Managing Cyber Risks in an Increasingly Outsourced World," ISSA SoCal Security Symposium, Costa Mesa, AZ, October 25, 2018.

- Speaker, "Updates, a Case Study & Legal Developments in Background Screening," NAPBS Webinar, April 3, 2018.
- Speaker, "Driving Records: Putting Your Compliance in Gear," NAPBS 2018 Mid-Year Legislative & Regulatory Conference, Arlington, VA, April 15-17, 2018.
- Speaker, "Effective Cyber Risk Management: Overcoming Common Mistakes," Troutman Sanders Webinar, April 24, 2018.
- Speaker, "Incident Response Plans: Avoiding Common Mistakes Through a Table Top Exercise," Security Media Group's Fraud & Breach Prevention Summit, Dallas, TX, April 24- 25, 2018.
- Speaker, "Equifax Breach – Are There Regulatory Gaps," American Bar Association Webinar, November 15, 2017.
- Speaker, "Opportunity Is Knocking: How to Be Strategic Rather Than Reckless in Higher-Risk Industries and Products," Third Party Payment Processors Association Executive Summit, Scottsdale, AZ, November 9, 2017.
- Speaker, "Governing Without Clear Standards," ASIS International 63rd Annual Seminar and Exhibits, Dallas, TX, September 25-28, 2017.
- Speaker, "Emerging Topics in Privacy and Security," ISSA Summit, Los Angeles, CA, May 18-19, 2017.
- Speaker, "Standard of Care," NetDiligence Cyber Risk and Privacy Liability Forum, Philadelphia, PA, June 5, 2017.
- Panelist, "A Case Study & Legal Developments in Background Screening," National Association of Professional Background Screeners Webinar, June 28, 2017.
- Speaker, "Governing Without Clear Standards: Lessons Learned From the Trenches," ISACA LA Spring Conference, Los Angeles, CA, April 12, 2017.
- Panelist, "Building Better Compliance to Defend Against Inaccuracy Claims: Lessons from Recent Wins," National Association of Professional Background Screeners Mid-Year Legislative & Regulatory Conference, Washington, DC, March 20, 2017.
- Speaker, "Governing Without Clear Standards: Lessons Learned From the Trenches," ISSA Puerto Rico Cybersecurity Conference, March 17, 2017.
- Panelist, "The Supreme Court's *Spokeo* Decision – A Busy Six Months," Troutman Sanders Consumer Financial Services Webinar Series, November 10, 2016.
- Panelist, "Financial Privacy and Data Security," American Bar Association National Institute Conference on Consumer Financial Services Basics, Arlington, VA, October 18, 2016.
- Panelist, "Cybersecurity," American Bar Association National Institute Conference on Consumer Financial Services Basics, Arlington, VA, October 18, 2016.
- Panelist, "Big Data in the Privacy Context: Impact of the FTC's Report on Use of Big Data and a Look into How Big Data Will Be Regulated in the Future," American Conference Institute's 20th Advanced Global Legal and Compliance Forum on Privacy & Security of Consumer and Employee Information, San Francisco, CA, October 13, 2016.
- Panelist, "Cybersecurity in Financial Institutions Industry," Troutman Sanders Consumer Financial Services Webinar Series, October 5, 2016.
- Panelist, "Class Actions: Data Privacy & Security Breach Case Law, Trends in Key Jurisdictions and Circuit Court Rulings, New Class Certification Issues, Novel Standing, Causation, Damages, Injury and Actual Harm Nuances, and ?How the *Spokeo* and *PF Chang* Decisions Will Change the Landscape,"

American Conference Institute's 2nd National Forum on Data Breach & Privacy Litigation and Enforcement, New York, NY, September 29, 2016.

- Panelist, "FCRA Compliance and Litigation Trends for Resellers," National Association of Professional Background Screeners Annual Conference, Palm Desert, CA, September 19, 2016.
- Panelist, "Working Toward Prevention of the Breach: What Do Phishing Incidents Look Like?;" "How Do Forensic Investigations Take Place?;" and "Are There Ways to Try to Prevent the Breach?," American Conference Institute's 13th National Forum on Cyber & Data Risk Insurance, New York, NY, July 28, 2016.
- Panelist, "Privacy and Security by Design: How to Fix Ineffective Governance Programs," American Conference Institute's 16th Advanced Global Legal & Compliance Forum on Cyber Security and Data Privacy & Protection, Chicago, IL, June 23, 2016.
- Panelist, "*Spokeo, Inc. v. Robins:* What are the Key Points for the Background Screening Industry?," National Association of Professional Background Screeners Webinar, June 14, 2016.
- Panelist, "Lessons Learned from 10 Years of Litigation," NetDiligence Cyber Risk & Privacy Liability Forum, Philadelphia, PA, June 7, 2016.
- Panelist, "Privacy vs. Security; Apple and the FBI," The Eighth Annual Information Security Summit, Los Angeles, CA, May 20, 2016.
- Speaker, "The Future Is Now; A Forum on Business and Legal Issues Related to FinTech," Fintech Event, New York, NY, May 19, 2016.
- Speaker, "Data Breach Litigation: How to Avoid It and Be Better Prepared for Defense," Troutman Sanders Consumer Financial Services Webinar Series, May 3, 2016.
- Speaker, "Class Actions: Minimizing Litigation Woes for Employers," FCRA, April 27, 2016.
- Panelist, "Working Toward Prevention of the Breach: What Do Phishing Incidents Look Like?;" "How Do Forensic Investigations Take Place?;" and "Are There Ways to Try to Prevent the Breach?," American Conference Institute Cyber & Data Risk Insurance Conference, Chicago, IL, April 1, 2016.
- Speaker, "Business to Business Claims: Vendor Lawsuits; Litigation Between Issuing Banks and Retailers Post-Breach; the Ecosystem of Payment Card Breaches; and Genesco Decision Implications," ACI Data Breach & Privacy Litigation and Enforcement Conference, March 17-18, 2016.
- Panelist, "Data Breach Litigation: How to Avoid It and Be Better Prepared for Defense," RSA Conference, San Francisco, CA, March 3, 2016.
- Panelist, "Deflecting the Onslaught: Data Breach Litigation Defenses & Litigation Against Responsible Third Parties," HB Data Breach & Privacy Litigation Conference, San Francisco, CA, February 11, 2016.
- Panelist, "Why Are Transnational Criminal Enterprises Targeting the Financial Services Sector and Is My Organization Prepared or Are We the Next Victim?," Information Systems Security Association, Webinar, February 5, 2016.
- Panelist, "Cyber Security Preparedness: Data Breach Incident Response Teams and Refurbishing Your Governance Programs," American Conference Institute 18th Advanced Global Legal & Compliance Forum on Cyber Security and Data Privacy & Protection, Washington, DC, January 29, 2016.
- Panelist, "FFIEC Cyber Security Assessment Tool (Assessment) for Financial Institutions: What You Need to Know in 2016 and Beyond," The Knowledge Group, January 28, 2016.
- Moderator, "FCRA Compliance," ABA Consumer Financial Services Winter Meetings, January 9-12, 2016.

- Panelist, "The Impact of Fair Credit Reporting Act in the Regulatory Enforcement and Developments of Financial Services," The Knowledge Group, November 16, 2015.
- Speaker, "Cyber Security Liability Insurance: Need It or Leave It," 2015 ISSA International Conference, October 11-13, 2015.
- Speaker, NetDiligence: Cyber Liability Conference West Coast, October 7, 2015.
- Speaker, "Incident Response Plans With a Focus on Governance Within an Organization," ACI: 17th Global Legal and Compliance Forum on Cyber Security and Data Privacy & Protection, October 2015.
- Speaker, "The Changing Landscape of Cyber Liability Litigation: Data Breach Class Actions and Impact on Assessing What Breaches and Resulting Claims are Worth," ACI 11th National Advanced Forum on Cyber & Data Risk Insurance, October 2015.
- Speaker, "Understanding the Cybersecurity Risk in Financial Institutions," ISSA Financial SIG Webinar, June 12, 2015.
- Speaker, "Data Governance in the Era of the Data Breach," NYS Cyber Security Conference, June 2, 2015.
- Speaker, "Lessons Learned and Tips from Fourteen FCRA Lawsuits Filed by One Plaintiff," NAPBS 2015 Mid-Year Legislative and Regulatory Conference, April 14, 2015.
- Speaker, "The Increased Importance of Sound Data Governance in the Data Breach Era," IAPP KnowledgeNet LA Chapter, April 9, 2015.
- Speaker, "The Whole Company Approach: Working with Your IT Department to Safeguard Networks, Data and Information," ACI Cyber & Data Risk Insurance, March 23, 2015.
- Speaker, "Class Actions & Litigation Roundup: Recent Data Breach Cases, Mega-Privacy Actions, TCPA and Texting Suits, and Assessing What Claims Are Worth," ACI Cyber Security & Data Privacy and Protection, January 15, 2015.
- Speaker, "Policy Driven Security – Deploy Only Those Security Technologies and Controls That You Need," ISMG Fraud Summit Dallas, November 18, 2014.
- Speaker, "What to Tell the Regulators (and Affected Customers) and When?" IAPP Practical Privacy Series New York, November 5-6, 2014.
- Speaker, "Increasing Importance of Data Governance in the Era of (Seemingly) Daily Data Breaches," NAPBS Speaker at 2014 Annual Conference, October 21, 2014.
- Speaker, "Advanced Cyber Coverage," HB Litigation Conferences Presents: The NetDiligence Cyber Risk & Privacy Liability Forum, October 8-9, 2014.
- Speaker, "Financial Privacy and Credit Reporting," ABA Fifth Annual National Institute on Consumer Financial Services Basics, October 6-7, 2014.
- Speaker, "The Whole Company Approach: Working With Your IT Department to Safeguard Networks, Data and Information," ACI 9th National Advanced Forum on Cyber & Data Risk Insurance, September 29-30, 2014.
- Speaker, "The ABCs of Data Security and Compliance: A Guide to Navigating Data Issues," Presentation to Asurion, Inc., September 12, 2014.
- Speaker, "Data Breach and Coverage Litigation," HB Litigation Conferences Presents: The NetDiligence Cyber Risk & Privacy Liability Forum, June 11-13, 2014.

- Speaker, "Retaliatory Hacking: Legitimate Corporate Defense?," NYS Cyber Security Conference, June 2-3, 2014.
- Speaker, "Fraud Summit," Information Security Media Group, May 24, 2014.
- Speaker, "Data Breach Litigation Update - Example Standing in Data Security Breach Cases," ACI 8th National Advanced Forum on Cyber & Data Risk Insurance, March 24-25, 2014.
- Speaker, "Anatomy of a Data Breach: What You Say (or Don't Say) Can Hurt You," RSA Conference 2014, February 24-28, 2014.
- Speaker, "Privacy in the Digital Age - Is There Even a Barn Door Left to Close?" ABA Presentation, February 6-9, 2014.
- Speaker, "Social Media for Business," HB Litigation Conferences LLC, November 14, 2013.
- Speaker, "Data Governance: How Strong Data Governance Addresses Big Data, BYOD, the Cloud and Other Issues," LexisNexis Webinar, November 14, 2013.
- Speaker, "*Daubert*: New Challenges New Opportunities," Nationwide, October 24, 2013.
- Speaker, "Litigation Round Up: Using Recent Cases and Class Actions Claims to Assess What Breaches & Resulting Claims Are Worth," ACI 7th Annual Advanced Summit on Cyber & Data Risk Insurance, September 30–October 1, 2013.
- Speaker, "Digital Media: Data Breach/Security/Privacy," No Brown Bag Series, September 11, 2013.
- Speaker, "Social Media," HB Litigation Webinar, September 9, 2013.
- Speaker, "Top Ten Suggestions for Effective Management of Complex Business Litigation and Class Actions," HB Litigation Webinar, September 3, 2013.
- Speaker, "*Daubert*: New Challenges; New Opportunities," Presentation to Nationwide, August 30, 2013.
- Speaker, "Data Breach: Public Relations and Notice Communication Issues," Thompson Routers, July 22, 2013.
- Speaker, "Dissecting a Data Breach Claim," HB Litigation Conferences Presents: NetDiligence Cyber Risk & Privacy Liability Forum, June 6-7, 2013.
- Speaker, "Litigation Outline Training," Presentation to LexisNexis, April 15 and May 17, 2013.
- Speaker, Concordance Partners in Excellence and LAW PreDiscovery User Group Conference, "Challenges Facing Corporations and Their Law Firms on eDiscovery," March 24, 2013.
- Speaker, "2013 Traffic Jam: The Intersection of Social Media, Privacy Laws and Data Security," Ohio Information Security Conference, March 17, 2013.
- Speaker, "Data Security and Privacy in the Age of Social Media and Employee-Owned Devices," Nationwide, December 17, 2012.
- Speaker, LexisNexis Emerging Issues Webinar Series, "2013 Traffic Jam: The Intersection of Social Media and Insurance," November 15, 2012.
- Speaker, "Welcome to Tomorrowland, Today - BYOD It's Here, Are you Ready?," ISSA International Conference, October 25-26, 2012.
- Speaker, HB Litigation Conferences Presents: NetDiligence Cyber Risk & Privacy Liability Forum, October 11-12, 2012.
- Speaker, "ABCs of Privacy," October 2, 2012.
- Speaker, ACI 6th Annual Advanced Summit on Cyber & Data Risk Insurance, September 27, 2012.

- Speaker, "Digital Media: Data Breach / Security / Privacy," Cincinnati Bar Association No Brown Bag Seminar, September 11, 2012.
- Speaker, "Managing Mobility: Minimizing Threats Posed by Mobile Devices, Applications and Workforces Through Proven Security Measures," ACI's 12th National Legal and Compliance Forum on Privacy & Security of Consumer and Employee Information, July 30-31, 2012.
- Speaker, "Post-Breach Communications Issues," Webinar, July 2012.
- Speaker, "Top Regulatory Issues for 2012: What Every Business Should Know," and "Data Security and Privacy in the Age of Social Media and Employee-Owned Devices," LexisNexis MCLE Forum, June 21, 2012.
- Presenter, "Top Regulatory Issues for 2012: What Every Business Should Know," and "Data Security and Privacy in the Age of Social Media and Employee-Owned Devices," Federal Express Ground, June 21, 2012.
- Speaker, "BYOD: Privacy and Security Issues to Consider Before Inviting Employee-Owned Devices," UD Seminar, June 8, 2012.
- Speaker, "Top Regulatory Issues for 2012: What Every Business Should Know," LexisNexis MCLE Forum, June 7, 2012.
- Speaker, "Vendor Management - How to Do it Well," HB Litigation Conferences Presents: NetDiligence Cyber Risk & Privacy Liability Forum, June 4-5, 2012.
- Speaker, "Privacy & Security of Consumer and Employee Information," ACI 11th Annual Legal and Compliance Forum, February 1-2, 2012.
- Presenter, Dodd-Frank Presentation to Federal Express, December 6, 2011.
- Presenter, Dodd-Frank Presentation to Nationwide, December 6, 2011.
- Speaker, "Damages and Other Litigation After a Data Breach," HB Litigation Conferences Presents: NetDiligence Cyber Risk & Privacy Liability Forum, October 4-5, 2011.
- Speaker, "Managing a Crisis: Panel Discussion on a Complex Data Breach Hypothetical," ACI, June 20, 2011.
- Speaker, "Solving Special Computer Security Issues," HB Litigation Conferences Presents: NetDiligence Cyber Risk & Privacy Liability Forum, June 9-10, 2011.
- Speaker, "Red Flags Rule Revisited - Beyond Financial Institutions," IAPP Audio Conference, August 6, 2009.
- Speaker, "Using Social Networking and Web 2.0 Sites in Trial Practice," NBI Teleconference, July 23, 2009.
- Speaker, "Legal Ethics in the Information Age," NBI Teleconference, January 27, 2009.
- Speaker, "Privacy and Data Protection - A Practical Guide," NBI Teleconference, December 19, 2008.
- Speaker, "The Top Ten Issues in Health Care Privacy," GDAHA Presentation, October 21, 2008.
- Speaker, "The Recent ID Theft Red Flag Regulations and Other Indicators to Help Organizations Build Defensible Data Protection and Compliance Programs," UD Seminar, June 6, 2008.
- Presenter, Association of Corporate Counsel, May, 15, 2008.
- Speaker, "E-Discovery: Now What?" NBI Seminar, May 7, 2008.
- Speaker, "Best Practices in E-Discovery Management," NBI Teleconference, December 28, 2007.

- Speaker, "Legal Ethics in the Information Age," NBI Teleconference, December 21, 2007.
- Speaker, "Find it Free and Fast on the Net: Strategies for Legal Research on the Web," NBI Seminar, August 2, 2007.
- Speaker, "Privacy and Compliance: Relevant to All Businesses," July 30, 2007.
- Speaker, "E-Discovery: Applying the New FRCP Changes," NBI Seminar, July 24, 2007.
- Speaker, "E-Discovery and Computer Forensics: Effectively Preserving Evidence," NBI Webinar, June 19, 2007.
- Speaker, "E-Discovery and Forensics: Effectively Preserving Evidence," NBI Webinar, December 7, 2006.
- Speaker, "E-Discovery and Computer Forensics: Strategies for Success," NBI Seminar, November 1, 2006.
- Speaker, "Internet Strategies for Legal Professionals," NBI Seminar, August 14, 2006.
- Speaker, "Intellectual Property, Privacy and Transactional Issues," UD Seminar, June 9, 2006.
- Speaker, "Basics of Civil Litigation (Pretrial); Defendant's Perspective," New Lawyer Training Seminar, December 16, 2005.
- Speaker, "Preparing, Presenting & Attacking a Damages Claim in Business Litigation," Faruki Ireland & Cox P.L.L. Damages Seminar, October 7, 2005.
- Speaker, "Digital Technology and the Law," NBI Seminars, September 14 & 28, 2005.
- Speaker, "Getting the Evidence You Need: Effectively Conducting E-Discovery and Computer Forensics in Ohio," NBI Seminar, June 13, 2005.
- Speaker, "Overcoming Your Fears: Utilizing Technology in Litigation," NBI Seminar, March 22, 2005.
- Speaker, "Document Gathering, Production and Management for Litigation Paralegals in Ohio," IPE Seminar, January 25, 2005.
- Speaker, "Protecting Your Ideas," i-Zone Presentation, January 12, 2005.
- Presenter, "Electronic Discovery: Top Ten List for Being Prepared," Presentation to The Reynolds & Reynolds Company, June 2002.
- Speaker, "Creating Your Business; Legal and Practical Considerations," i-Zone Presentation, February 2002.
- Speaker, "December 2000 Amendments to Federal Rules," CLE Seminar, February 9, 2001.

## Publications

- Co-author, "California Delete Act: An Aggressive New Approach to Regulating Data Brokers," *Troutman Pepper*, October 19, 2023.
- Co-author, "CFPB Outlines Rulemaking Plan to Dramatically Alter Decades of FCRA Requirements for Everyone in the Consumer Data Ecosystem," *Troutman Pepper*, September 21, 2023.
- Co-author, "Impending FCRA Data Broker Rulemaking Announced by CFPB Director Chopra at White House Data Broker Roundtable," *Troutman Pepper*, August 16, 2023.
- Co-author, "CPRA Shuffle: Two Steps Forward, One Step Back: Court Temporarily Halts CPRA Regulation Enforcement as CPRA Enforcements Begins," *Troutman Pepper*, July 21, 2023.

- Podcast, "AI: Impact and Use in Background Screening (Part Five)," *Regulatory Oversight* Podcast, May 30, 2023.
- Co-author, "Cookies and Online Tracking of Health Signals: An OCR Prescription for Potential Peril," *Troutman Pepper*, May 4, 2023.
- Co-author, "Washington Legislature Goes Big With "My Health My Data Act"," *Troutman Pepper*, May 2, 2023.
- Co-author, "Iowa on Cusp of Enacting Privacy Legislation," *Troutman Pepper*, March 22, 2023.
- Co-author, "California Age-Appropriate Design Code Is Not Child's Play - Five Practical Tips to Comply and Protect Kids' Privacy," *Pratt's Privacy & Cybersecurity Law Report*, January 2023.
- Co-author, "CFPB Highlights Purported "Problems With Tenant Background Checks"," *Troutman Pepper*, November 18, 2022.
- Co-author, "Ad Technology Compliance Tips From Video Privacy Claims," *Law360*, October 19, 2022.
- Co-author, "California Age-Appropriate Design Code Is Not Child's Play - Five Practical Tips to Comply and Protect Kids' Privacy," *Troutman Pepper*, October 4, 2022.
- Co-author, "Four Strategies for Drafting Effective Consumer Breach Notices," *Law360*, September 30, 2022.
- Co-author, "Deadline for New UK Contract Requirements for Personal Data Transfers Is Here (EU and California Deadlines Looming)!," *Troutman Pepper*, September 27, 2022.
- Co-author, "Piecing It All Together: OFAC Combines Seven Years of Regulations, Amendments, and Interpretations All in One," *Troutman Pepper*, September 14, 2022.
- Co-author, "Compliance Lessons From Sephora CCPA Settlement," *Law360*, September 13, 2022.
- Co-author, "CCPA/CPRA Will Apply to Employee AND B2B Data — Five Steps to Prepare for the January 1, 2023 Effective Date," *Troutman Pepper*, September 6, 2022.
- Co-author, "Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements," *Troutman Pepper*, August 30, 2022.
- Co-author, "The Do's and Don'ts of Cybersecurity Forensic Investigations," *Law360*, August 26, 2022.
- Co-author, "CPRA Draft Regulations: Essential Takeaways and Ten Actions to Take Now," *Hedge Fund Law Report*, August 25, 2022.
- Co-author, "California ADCA Bill Aims to Increase Children's Data Privacy," *Security Magazine*, August 24, 2022.
- Co-author, "Simplifying a Complicated Process — Four Steps to Comply with China's PIPL New Security Assessment Requirements for Cross-Border Data Transfers September 1, 2022," *Troutman Pepper*, August 9, 2022.
- Co-author, "CPRA Draft Regulations: Essential Takeaways and 10 Actions to Take Now," *Cybersecurity Law Report*, July 13, 2022.
- Co-author, "Focusing on the Primary Purpose: Protecting the Attorney–Client Privilege and Work Product Doctrine in Incident Response," *Cyber Security: A Peer-Reviewed Journal*, July 11, 2022.
- Co-author, "California Privacy Protection Agency Publishes Draft Rules," *Troutman Pepper*, June 6, 2022.
- Co-author, "CPRA Series: Part Four – Data Processing Obligation," *Daily Journal*, May 23, 2022.

- Co-author, "CPRA Series: Part Three – Notice and Disclosure Obligations," *Daily Journal*, May 12, 2022.
- Co-author, "Ninth Circuit Provides Guidance on Web Scraping," *Troutman Pepper*, May 5, 2022.
- Co-author, "Connecticut Legislature Passes Comprehensive Privacy Legislation, Awaiting Governor's Signature," *Troutman Pepper*, May 4, 2022.
- Co-author, "CPRA Series: Part Two – Consumer Rights," *Daily Journal*, April 20, 2022.
- Co-author, "Federal Contractors on Notice After DOJ Announces First Civil Cyber Fraud Initiative Settlement," *Troutman Pepper*, April 21, 2022.
- Co-author, "CPRA Series: Part One – Introduction and Overview," *Daily Journal*, April 11, 2022.
- Co-author, "A Fresh "Face" of Privacy: 2022 Biometric Laws," *Troutman Pepper*, April 5, 2022.
- Co-author, "US and Europe Issue Joint Statement Announcing Agreement on New Trans-Atlantic Data Privacy Framework to Replace EU-US Privacy Shield," *Troutman Pepper*, March 28, 2022.
- Co-author, "Utah Becomes Fourth State to Adopt Privacy Legislation," *Troutman Pepper*, March 24, 2022.
- Co-author, "Credit Bureaus Dramatically Reduce Medical Debt Credit Reporting," *Troutman Pepper*, March 22, 2022.
- Co-author, "2021 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Pepper*, January 28, 2022.
- Co-author, "First Amendment Challenge to Restriction on Public Access to Electronic Court Records Advances," *Troutman Pepper*, January 18, 2022.
- Co-author, "Tenant Screening Receiving Increased Federal Regulatory and Legislative Focus," *Professional Background Screening Association Journal*, November/December 2021.
- Co-author, "Think Fast: Banking Regulators Release Final Computer-Security Incident Notification Requirements," *Troutman Pepper*, December 2, 2021.
- Co-author, "U.K. Supreme Court Finds Data Protection Representative (*I.e.*, Class) Action Cannot Be Pursued Against Google," *Troutman Pepper*, November 29, 2021.
- Co-author, "CFPB Issues Advisory Opinion on Name-Only Matching," *Troutman Pepper*, November 5, 2021.
- Co-author, "App Store 'Nutrition Labels' Raise New Privacy Risks for Cos.," *Law360*, October 22, 2021.
- Co-author, "Delaware Court of Chancery Highlights Seriousness of Cybersecurity Concerns While Maintaining High Standard for Caremark Claims," *Troutman Pepper*, October 12, 2021.
- Co-author, "Sued for a Data Breach Out of State? Don't Forget a Personal Jurisdiction Defense," *Pratt's Privacy & Cybersecurity Law Report*, October 2021, Vol. 7, No. 8.
- Co-author, "New UK Standards for Children's Digital Services Take Effect — Provides Framework for New US Law," *Troutman Pepper*, September 23, 2021.
- Co-author, "Movement on All Sides Toward Broader Data Privacy and Security Oversight by FTC," *Troutman Pepper*, September 20, 2021.
- Co-author, "Top Takeaways From a Year of CCPA Enforcement," *Bloomberg Law*, August 6, 2021.
- Co-author, "Connecticut Passes Stronger Data Breach Notification and Cybersecurity Liability Statutes," *Troutman Pepper*, July 19, 2021.

- Co-author, "Colorado Governor Enacts Comprehensive Data Privacy Bill — How Does It Compare to California and Virginia?," *Troutman Pepper*, July 14, 2021.
- Co-author, "CFPB Issues Bulletin on Rental Screening and Issues of Concern," *Troutman Pepper*, July 7, 2021.
- Co-author, "Supreme Court Decision: *TransUnion v. Ramirez*," *Troutman Pepper*, June 25, 2021.
- Co-author, "Colorado Passes Comprehensive Data Privacy Law," *Troutman Pepper*, June 15, 2021.
- Co-author, "Litigation and Enforcement: Virginia Consumer Data Protection Act Series (Part Five)," *Troutman Pepper*, April 1, 2021.
- Co-author, "Supreme Court Considers Standing and Typicality for No-Injury Class Actions in *TransUnion v. Ramirez Oral Argument*," *Troutman Pepper*, March 31, 2021.
- Co-author, "Data Processing Obligations: Virginia Consumer Data Protection Act Series (Part Four)," *Troutman Pepper*, March 25, 2021.
- Co-author, "California Court Tosses Alleged "Data Breach" Suit, Holding CCPA Does Not Apply Retroactively," *Troutman Pepper*, March 24, 2021.
- Co-author, "Notice and Disclosure Obligations: Virginia Consumer Data Protection Act Series (Part Three)," *Troutman Pepper*, March 18, 2021.
- Co-author, "California AG Announces Approval of Fourth Set of Modifications to CCPA Regulations," *Troutman Pepper*, March 16, 2021.
- Co-author, "Consumer Rights: Virginia Consumer Data Protection Act Series (Part Two)," *Troutman Pepper*, March 11, 2021.
- Co-author, "Circuit Split on Class Feasibility Offers Defense Opportunities," *Law360*, March 8, 2021.
- Co-author, "Introduction and Overview: Virginia Consumer Data Protection Act Series (Part One)," *Troutman Pepper*, March 4, 2021.
- Co-author, "Data Compliance Issues for Cos. Making, Using Vaccine App," *Law360*, February 10, 2021.
- Co-author, "CCPA's Employee and Business-to-Business Information Exemptions Extended Until at Least January 1, 2022," *Troutman Pepper*, September 1, 2020.
- Co-author, "Employers' Top 7 Coronavirus Data Collection Questions," *Law360*, June 15, 2020.
- Co-author, "Calif. Privacy Law Takeaways From 9th Circ. Facebook Case," *Law360*, April 27, 2020.
- Co-author, "Privacy Guidelines for COVID-19 Contact-Tracing App Makers," *Law360*, April 17, 2020.
- Co-author, "COVID-19 Warrants Modified Cybersecurity for Work-At-Home," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Cybersecurity Tips to Prevent Your Business From Becoming COVID-19's Virtual Victim," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Notice to Employers: Remember Privacy Basics When Addressing COVID-19," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Request for Assurance From Critical Vendors of Operational Preparedness to Address COVID-19," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Calif. AG's Latest Privacy Law Revisions Miss Some Spots," *Law360*, March 19, 2020.
- Co-author, "INSIGHT: FTC Report Offers Road Map to Mitigate CCPA Data Breach Class Actions," *Bloomberg Law*, March 5, 2020.

- Co-author, "Ninth Circuit Holds All Class Members in Rule 23 Class Must Have Standing at Final Judgment to Recover Monetary Damages and Affirms Multi-Million Dollar FCRA Jury Verdict," *Troutman Sanders*, March 2, 2020.
- Co-author, "2019 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Sanders*, February 24, 2020.
- Co-author, "CCPA Modified Draft Regulations: Two Steps Forward, One Step Back," *The Recorder*, February 10, 2020.
- Co-author, "INSIGHT: First CCPA-Related Case Foreshadows Five Issues," *Bloomberg Law*, February 10, 2020.
- Co-author, "'Data Brokers' Must Register With the California Attorney General by Tomorrow, January 31st," *Troutman Sanders*, January 30, 2020.
- Co-author, "Ill. Privacy Bill Is Not as Robust as Calif. Law," *Law360*, December 17, 2019.
- Co-author, "INSIGHT: Five Reasons to Comment on Draft CCPA Regulations," *Bloomberg Law*, October 22, 2019.
- Co-author, "Calif. Privacy Law Means New Approach to Vendor Contracts," *Law360*, September 27, 2019.
- Co-author, "INSIGHT: So the CCPA Is Ambiguous—Now What?," *Bloomberg Law*, June 14, 2019.
- Co-author, "Data Privacy: Developments in Regulatory Enforcement," *Pratt's Privacy & Cybersecurity Law Report*, *LexisNexis*, January 2019.
- Co-author, "Data Privacy: The Current Legal Landscape 2018 Reviewed," *Troutman Sanders News & Knowledge*, January 15, 2019.
- Co-author, "Data Privacy: Developments in Regulatory Enforcement," *Pratt's Privacy & Cybersecurity Law Report - Lexis Nexis*, January 2019.
- Author, "Data Privacy: The Current Legal Landscape – September 2018," *Troutman Sanders News & Knowledge*, September 26, 2018.
- Co-author, "Clarity on Overlapping Background Check Laws in Calif.," *Law360*, August 22, 2018.
- Co-author, "Annual Report: 2017 Consumer Financial Services Year in Review and a Look Ahead," January 10, 2018.
- Co-author, "Top Data Governance Issues From 2017 and What to Watch in 2018," *The National Law Review*, January 9, 2018.
- Author, "Data Privacy: The Current Legal Landscape – Annual Edition," *Troutman Sanders News & Knowledge*, February 10, 2017.
- Author, "Data Privacy: The Current Legal Landscape – Quarterly Update, October 2016," *Troutman Sanders News & Knowledge*, November 4, 2016.
- Co-author, "Data Breach Defenses When Consumer Plaintiffs Come Knocking," *Lexis Nexis,* August 15, 2016.
- Author, "Practical Advice on Applying for the EU-U.S. Privacy Shield Program," *Troutman Sanders News & Knowledge*, July 29, 2016.
- Co-author, "The Technology Lawyer and Connected Things," *Law360*, July 28, 2016.
- Co-author, "Underwriting in an Even More Connected World," *PLUS Journal*, March 2016.

- Co-author, "Data Privacy: The Current Legal Landscape," March 2, 2016.
- Author, "To Address Cyber Vulnerability, Address the Human Factor," *Daily Journal*, October 29, 2015.
- Author, "Ten Years Later: Data Governance in the Decade of the Data Breach," September 2015.
- Author, "BYOD Bring Your Own Device (Know The Privacy and Security Issues Before Inviting Employee Owned Devices to the Party)," April 2012.
- Author, "Getting Support for Privacy and Data Compliance: Not a Hard Sell if Done Right," October 2011.
- Author, "Encryption Technologies May Not Be Optional," December 2008.
- Author, "Data Security and Ethical Hacking; Points to Consider for Eliminating Avoidable Exposure," September/October 2008.
- Author, "Privacy in the Office," August 2008.
- Author, "The Recent ID Theft Red Flag Regulations and Other Indicators to Help Organizations Build Defensible Data Protection and Compliance Programs," June 2008.
- Author, "There Has Been a Data Security Breach: But Is Notice Required?" December 2007.
- Author, "de fin ing – Data Security Measures That Protect Your Company and Customers," December 2007.
- Author, "Data Security Breaches: Defining Measures Appropriate Under the Circumstances," December 2007.
- Author, "Preparing for the Rule 2669 Scheduling Conference and Other Practical Advice in the Wake of the Recent Amendments to the Rules Governing E-Discovery," August 2007.
- Author, "E-Discovery and Computer Forensics: Effectively Preserving Evidence," December 2006.
- Author, "Security Before and After a Data Breach," November/December 2006.
- Author, "E-Discovery and Computer Forensics: Strategies for Success," November 2006.
- Author, "Sarbanes-Oxley & Internal Controls: The Not So Hidden Implications for Information Technology and Information Security," September 2006.
- Author, "Internet Strategies for Legal Professionals," August 2006.

## Media Commentary

- Quoted, "CFPB Outlines Sweeping Data Proposal, Drawing Swift Bank Condemnation," *American Banker*, September 21, 2023.
- Interviewed, "Protecting CISOs From Taking the Blame," *BankInfoSecurity*, April 26, 2023.
- Quoted, "Website-Tracking Lawsuits: A Guide to New Video Privacy Decisions Starring PBS and People.com," *Cybersecurity Law Report*, March 29, 2023.
- Quoted, "Top Privacy Developments of 2022: Midyear Report," *Law360*, July 22, 2022.
- Interviewed, "Legal and Litigation Trends in 2022," *Information Security Media Group*, June 20, 2022.
- Quoted, "Kroger Reaches $5M Settlement With Breach Victims, as Supreme Court Defines 'Actual Harm'," *SC Magazine*, July 8, 2021.

- Quoted, "Kroger, British Airways Agree to Settle Data Breach Lawsuits," *Healthcare Info Security*, July 6, 2021.
- Quoted, "Vaccination Passports Are New Flashpoint in Covid-19 Pandemic," *The Wall Street Journal*, April 9, 2021.
- Quoted, "State Data Privacy Laws Pose Compliance Headaches for Banks," *American Banker*, March 8, 2020.
- Quoted, "Data Privacy Law's Biggest Challenge? Going Too Broad. Or Too Specific.," *Law.com*, April 2, 2020.
- Quoted, "Privacy Framework Faces Uphill Climb to Universal Adoption," *Law360*, February 21, 2020.
- Mentioned, "Tax Prep Co. Gets Final OK for $3M Data Breach Settlement," *Law360*, October 7, 2019.
- Quoted, "Vermont Law Rings in Registration, Disclosure for Data Brokers," *Bloomberg Law*, December 27, 2018.

## Professional and Community Involvement

- American Bar Association
- Federal Bar Association
- Ohio State Bar Association
- International Association of Privacy Professionals – CIPP/US Certified

## Rankings and Recognitions

- AV Rating® by Martindale Hubbell
- *Best Lawyers in America®:* Commercial Litigation (2013-2024)
- Lexology Legal Influencer for Q2 2020, Telecommunications, Media and Technology (TMT) – US
- Recognized as a Rising Star by *Super Lawyers,* 2005-2007
- Recognized as Ohio *Super Lawyer*, 2010-2013, 2015
- *Dayton Business Journal* Best of Bar, 2005, 2006
- Dayton Chamber of Commerce - Leadership Dayton Class of 2006
- 2003 *Dayton Business Journal* 40 Under 40 Award

## Professional Experience

- Adjunct professor at UD School of Law, 2001-2005.

## Bar Admissions

- California
- Ohio
- Minnesota

## Court Admissions

- Supreme Court of California
- Supreme Court of Minnesota
- Supreme Court of Ohio
- Supreme Court of the United States
- U.S. District Court, Central District of California
- U.S. District Court, Eastern District of California
- U.S. District Court, Northern District of California
- U.S. District Court, Southern District of California
- U.S. District Court, District of Colorado
- U.S. District Court, Eastern District of Michigan
- U.S. District Court, Middle District of North Carolina
- U.S. District Court, Northern District of Ohio
- U.S. District Court, Southern District of Ohio
- U.S. District Court, Eastern District of Wisconsin
- U.S. District Court, Western District of Wisconsin
- U.S. Court of Appeals, Second Circuit
- U.S. Court of Appeals, Fourth Circuit
- U.S. Court of Appeals, Fifth Circuit
- U.S. Court of Appeals, Sixth Circuit
- U.S. Court of Appeals, Seventh Circuit
- U.S. Court of Appeals, Eighth Circuit
- U.S. Court of Appeals, Ninth Circuit
- U.S. Court of Appeals, Tenth Circuit
- U.S. Court of Appeals, Eleventh Circuit

## Education

- University of Dayton, J.D., *magna cum laude*, 1996, associate editor, *Law Review*
- The Ohio State University, B.A., *cum laude*, 1992

## Clerkships

- Hon. Adele Riley, Montgomery Common Pleas Court, Ohio, 1995 - 1995
- Hon. Jack Meagher, Montgomery Common Pleas Court, Ohio, 1994 - 1995

## Sadia Mirza

Partner
Orange County

sadia.mirza@troutman.com
D 949.622.2786


Sadia leads the firm's Incidents + Investigations team, advising clients on all aspects of data security and privacy issues. She is the first point of contact when a security incident or data breach is suspected, and plays a central role in her clients' cybersecurity strategies.

**Areas of Focus:**

- Privacy + Cyber
- Financial Services Litigation
- Consumer Financial Services
- Advanced Technology: Leading-Edge Issues
- Incidents + Investigations

Sadia's practice is dedicated to counseling clients on complex data security and privacy issues. Capitalizing on her extensive experience guiding clients through security incidents, she handles pre-incident planning and readiness, breach investigations, and litigation matters. Sadia leverages her 360-degree knowledge of the incident response lifecycle to ensure clients can present a positive and defensible narrative to plaintiffs or regulators.

Clients also turn to Sadia for best practices related to privacy compliance and novel data-use questions and concerns. An active and respected voice in the privacy and data security bar, she writes and speaks frequently on trends and developments affecting clients and consumers. Sadia has been a panelist on numerous privacy and cybersecurity panels across the U.S. and is a member of the Program Committee for the Law Track for the RSA Conference.

Sadia provides ongoing analysis and commentary on developments in the consumer financial services industry, with a focus on privacy law, through the Consumer Financial Services Law Monitor blog at cfslawmonitor.com. She frequently publishes in *Bloomberg Law* and *Law360*.

Sadia is a Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Manager (CIPM).

## Representative Matters

- Serving as counsel for a Software as a Service (SaaS) provider in one of the first class actions alleging CCPA violations and other privacy-based claims.
- Serving as counsel for a SaaS provider in a Multidistrict litigation (MDL) for claims related to a 2020 ransomware attack.
- Representing a SaaS provider in interactions with state attorneys general and other state governmental bodies in connection with a ransomware attack.
- Defended and represented companies that were the victims of Magecart attacks including by guiding them through Payment Card Industry (PCI) investigations.
- Serving as CCPA compliance counsel for multiple CRAs, public record vendors, data and analytics providers, and innovative technology companies.
- Prepared CCPA data inventory questionnaires for a wide variety of clients and conducted follow-up calls to review and enhance responses.
- Counseled innovative technology companies, advertising technology companies, financial institutions, and others with respect to various initiatives and product launches on issues relating to consumer protection and privacy, transactions, and compliance.
- Defended technology companies in class actions that challenged their data protection practices and asserted claims under various consumer protection statutes.
- Counsels a consumer reporting agency in all matters and activities concerning compliance with the FCRA, including the creation and revision of screening contracts and onboarding procedures.
- Created a compliance management system for a financial institution in a high-stakes and time-sensitive matter.

***Representative matters may include engagements before joining Troutman Pepper.***

## Related Practices and Industries

- Privacy + Cyber
- Financial Services Litigation
- Consumer Financial Services
- Advanced Technology: Leading-Edge Issues
- Class Action
- Consumer Reporting Agencies + Background Screening
- Data + Privacy
- Fair Credit Reporting Act (FCRA)
- Litigation + Trial
- Incidents + Investigations
- Corporate Espionage Response Team

## Speaking Engagements

- Speaker, "Resilience by Design," University of San Diego Center for Cyber Security Engineering and Technology 2023 Cyber Law & Risk Symposium, November 2, 2023.
- Moderator, "International Regulatory & Litigation Update," NetDiligence® Cyber Risk Summit, October 18, 2023.
- Panelist, CISO/CSO/General Counsel Summit, Converge Security, Anaheim, CA, September 15, 2023.
- Speaker, "Transforming Incident Response," NetDiligence Cyber Risk Summit, May 31, 2023.
- Speaker, "2022 Privacy and Cybersecurity Litigation, Legislative, and Enforcement Overview," Pennsylvania Bar Institute's 2023 Health Law Institute, March 15, 2023.
- Speaker, "California Workplace Developments and Preparing for 2023," Troutman Pepper, December 8, 2022.
- Panelist, "Emerging Trends with Cyber Security Threats: Effective Tactics to Assess, Prepare and Respond," Troutman Pepper and Aon Stroz Friedberg, October 19, 2022.
- Speaker, "A "Reasonable" Approach to Data Security," Privacy + Security Academy, November 3, 2022.
- Speaker, "Trifecta of Cybersecurity Resilience," Avertium and Troutman Pepper, September 29, 2022.
- Panelist, "Third-Party Vendor Breaches and IR Considerations that Follow," ePlace Solutions Cybersecurity Webinar, July 22, 2022.
- Panelist, "U.S. Litigation Update," NetDiligence Cyber Risk Summit, July 21, 2021.
- Panelist, "What Constitutes Reasonable Measures to Protect Confidential Information," ABA Program Webinar, July 20, 2022.
- Panelist, "U.S. Litigation and Regulatory Update," Cyber Risk Summit - Philadelphia, July 14, 2021.
- Panelist, "The Evolving Roles of Claims Professionals & Breach Coaches in Incident Response," NetDiligence Cyber Risk Summit, June 2, 2022.
- Panelist, "Cross Your Ts, but Watch Your Eyes – How to Improve Incident Response," 2021 ISACA Los Angeles Conference, April 13, 2021.
- Speaker, "Tabletop Exercises for Your Incident Response Plan," Privacy Week Forums 2021, January 28, 2021.
- Panelist, "Five Key Developments in the Privacy and Data Security Sector in 2020 and Five Predictions for 2021," Troutman Pepper webinar, January 26, 2021.
- Speaker, "2021: The Cybersecurity Legal, Privacy and Compliance Outlook," Bank Info Security, November 18, 2020.
- Speaker, "The Legal Outlook: Incident Response, Ransomware and CCPA," Bank Info Security, November 2, 2020.
- Speaker, "2021: The Cybersecurity Legal and Compliance Outlook," Bank Info Security, October 6, 2020.
- Presenter, "Privacy: The Current Status of the CCPA and Compliance Challenges," Troutman Pepper Webinar, August 11, 2020.

- Presenter, "COVID-19: CCPA and Regulatory and Governmental Litigation Update," Troutman Sanders Webinar, May 7, 2020.
- Moderator, "Quick Answers to Critical COVID-19 Compliance Questions for Financial Services Companies," Troutman Sanders Webinar, March 31, 2020.
- Speaker, "Incident Response Plans: Global Compliance Mandates and Obligations," ISMG Fraud & Breach Summit, December 3, 2019.
- Speaker, "The CCPA: It's Finally Ducking Here," Troutman Sanders, San Francisco, CA, January 16, 2020.
- Panelist, "Countdown to CCPA," IG3 Retreat Series, Newport Beach, CA, December 12, 2019.
- Speaker, "Getting Ready for 2020: Employment and Privacy Law Breakfast Seminar," Troutman Sanders, San Diego, CA, December 12, 2019.
- Speaker, "Getting Ready for 2020: Employment and Privacy Law Breakfast Seminar," Troutman Sanders, Orange County, CA, December 11, 2019.
- Speaker, "Partnering With Law Enforcement: Response and Investigative Strategies," Bank Info Security, November 18, 2019.
- Speaker, "CCPA: Less than Three Months 'Till Takeoff," CCPA ISACA, Orange County Forum, November 14, 2019.
- Speaker, "CCPA: Less Than Three Months 'Till Takeoff," Association of Continuity Professionals, Orange County Chapter Meeting, November 13, 2019.
- Speaker, "Getting Your Ducks in a Row for the California Consumer Privacy Act," Receivables Managements Association International Webinar, October 23, 2019.
- Speaker, "Amendments to the CCPA: The More Things Change, The More Things Stay the Same," Celesq Webinar, October 21, 2019.
- Panelist, "Cyber Resiliency Beyond Data Protection," NetDiligence Cyber Risk Summit, Santa Monica, CA, October 15-17th, 2019.
- Panelist, "Financial Privacy and Security," American Bar Association National Institute on Consumer Financial Services Basics, Nashville, TN, October 3, 2019.
- Speaker, "Fireside Chat: The CCPA and the Innovation Landscape," 34th Annual SoCal Security Symposium, Costa Mesa, CA, September 12, 2019.
- Speaker, "Getting Your Ducks in a Row for the California Consumer Privacy Act," Celesq Attorneys Ed Center, June 27, 2019.
- Speaker, "Incident Response Plans: Global Compliance Mandates and Obligations," ISMG Fraud and Breach Summit, Chicago, IL, May 14, 2019.
- Speaker, "Incident Response Plans: Global Compliance Mandates and Obligations," Bank Info Security, March 2, 2019.
- Speaker, "Getting Your Ducks in a Row for the California Consumer Privacy Act," Troutman Sanders Webinar, February 28, 2019.
- Speaker, "Consumer Financial Services Outlook 2019," Troutman Sanders Webinar, February 12, 2019.

## Publications

- Co-author, *Cyber Capsule*.
- Co-host, *Unauthorized Access* Podcast.
- Co-author, "California Delete Act: An Aggressive New Approach to Regulating Data Brokers," *Troutman Pepper*, October 19, 2023.
- Co-author, "Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter," *Reuters* and *Westlaw Today*, October 16, 2023.
- Co-author, "Data Protection: One of These Incidents Is Not Like the Other," *Reuters* and *Westlaw Today*, August 24, 2023.
- Co-author, "SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on their Security and Disclosure Plans," *Troutman Pepper*, July 31, 2023.
- Co-author, "CPRA Shuffle: Two Steps Forward, One Step Back: Court Temporarily Halts CPRA Regulation Enforcement as CPRA Enforcements Begins," *Troutman Pepper*, July 21, 2023.
- Co-author, "A Checklist for Cyber Incident Response Communications," *Law360*, July 14, 2023.
- Co-author, "Iowa on Cusp of Enacting Privacy Legislation," *Troutman Pepper*, March 22, 2023.
- Co-author, "Preparing for an Era of Regulated Artificial Intelligence," *Law360*, January 25, 2023.
- Co-author, "January 2023 Tech Tip - How to Know if You Should Consult a Breach Coach," *Orange County Bar Association*, January 10, 2023.
- Co-author, "A Little Breathing Room — California Privacy Agency Modifies Proposed Regulations," *Reuters*, December 8, 2022.
- Co-author, "Forensic Artifacts Play Legal Role in Cyber Incident Response," *Law360*, December 2, 2022.
- Co-author, "Silver Lining for Cos. in Proposed Calif. Privacy Law Changes," *Law360*, November 23, 2022.
- Co-author, "Cybersecurity Awareness Month - October 2022," *DBA Digest*, October 7, 2022.
- Co-author, "Cybersecurity Awareness Month - October 2022," *Troutman Pepper*, October 4, 2022.
- Co-author, "Four Strategies for Drafting Effective Consumer Breach Notices," *Law360*, September 30, 2022.
- Co-author, "Piecing It All Together: OFAC Combines Seven Years of Regulations, Amendments, and Interpretations All in One," *Troutman Pepper*, September 14, 2022.
- Co-author, "Compliance Lessons From Sephora CCPA Settlement," *Law360*, September 13, 2022.
- Co-author, "CCPA/CPRA Will Apply to Employee AND B2B Data — Five Steps to Prepare for the January 1, 2023 Effective Date," *Troutman Pepper*, September 6, 2022.
- Co-author, "Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements," *Troutman Pepper*, August 30, 2022.
- Co-author, "The Do's and Don'ts of Cybersecurity Forensic Investigations," *Law360*, August 26, 2022.
- Co-author, "CPRA Draft Regulations: Essential Takeaways and Ten Actions to Take Now," *Hedge Fund Law Report*, August 25, 2022.

- Co-author, "CPRA Draft Regulations: Essential Takeaways and 10 Actions to Take Now," *Cybersecurity Law Report*, July 13, 2022.
- Co-author, "Focusing on the Primary Purpose: Protecting the Attorney–Client Privilege and Work Product Doctrine in Incident Response," *Cyber Security: A Peer-Reviewed Journal*, July 11, 2022.
- Co-author, "California Privacy Protection Agency Publishes Draft Rules," *Troutman Pepper*, June 6, 2022.
- Co-author, "CPRA Series: Part Four – Data Processing Obligation," *Daily Journal*, May 23, 2022.
- Co-author, "CPRA Series: Part Three – Notice and Disclosure Obligations," *Daily Journal*, May 12, 2022.
- Co-author, "Ninth Circuit Provides Guidance on Web Scraping," *Troutman Pepper*, May 5, 2022.
- Co-author, "Connecticut Legislature Passes Comprehensive Privacy Legislation, Awaiting Governor's Signature," *Troutman Pepper*, May 4, 2022.
- Co-author, "CPRA Series: Part Two – Consumer Rights," *Daily Journal*, April 20, 2022.
- Co-author, "CPRA Series: Part One – Introduction and Overview," *Daily Journal*, April 11, 2022.
- Co-author, "Utah Becomes Fourth State to Adopt Privacy Legislation," *Troutman Pepper*, March 24, 2022.
- Co-author, "Déjà Vu? Outcomes of Privacy Legislation in 2022 State Legislative Sessions," *Troutman Pepper*, March 22, 2022.
- Co-author, "2021 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Pepper*, January 28, 2022.
- Co-author, "The Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Draft Connecticut Privacy Legislation: An Overview and Practical Guide," *The National Law Review*, November 2021.
- Co-author, "App Store 'Nutrition Labels' Raise New Privacy Risks for Cos.," *Law360*, October 22, 2021.
- Co-author, "Top Takeaways From a Year of CCPA Enforcement," *Bloomberg Law*, August 6, 2021.
- Co-author, "Litigation and Enforcement: Virginia Consumer Data Protection Act Series (Part Five)," *Troutman Pepper*, April 1, 2021.
- Co-author, "Data Processing Obligations: Virginia Consumer Data Protection Act Series (Part Four)," *Troutman Pepper*, March 25, 2021.
- Co-author, "California Court Tosses Alleged "Data Breach" Suit, Holding CCPA Does Not Apply Retroactively," *Troutman Pepper*, March 24, 2021.
- Co-author, "Notice and Disclosure Obligations: Virginia Consumer Data Protection Act Series (Part Three)," *Troutman Pepper*, March 18, 2021.
- Co-author, "Consumer Rights: Virginia Consumer Data Protection Act Series (Part Two)," *Troutman Pepper*, March 11, 2021.
- Co-author, "Introduction and Overview: Virginia Consumer Data Protection Act Series (Part One)," *Troutman Pepper*, March 4, 2021.
- Co-author, "Data Compliance Issues for Cos. Making, Using Vaccine App," *Law360*, February 10, 2021.
- Co-author, "Employers' Top 7 Coronavirus Data Collection Questions," *Law360*, June 15, 2020.
- Co-author, "Calif. Privacy Law Takeaways From 9th Circ. Facebook Case," *Law360*, April 27, 2020.

- Co-author, "Privacy Guidelines For COVID-19 Contact-Tracing App Makers," *Law360*, April 17, 2020.
- Co-author, "COVID-19 Warrants Modified Cybersecurity for Work-At-Home," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Cybersecurity Tips to Prevent Your Business from Becoming COVID-19's Virtual Victim," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Notice to Employers: Remember Privacy Basics When Addressing COVID-19," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Request for Assurance from Critical Vendors of Operational Preparedness to Address COVID-19," *International Association of Privacy Professionals*, April 2020.
- Co-author, "Calif. AG's Latest Privacy Law Revisions Miss Some Spots," *Law360*, March 19, 2020.
- Co-author, "INSIGHT: FTC Report Offers Road Map to Mitigate CCPA Data Breach Class Actions," *Bloomberg Law*, March 5, 2020.
- Co-author, "2019 Consumer Financial Services Year in Review & a Look Ahead," *Troutman Sanders*, February 24, 2020.
- Co-author, "CCPA Modified Draft Regulations: Two Steps Forward, One Step Back," *The Recorder*, February 10, 2020.
- Co-author, "INSIGHT: First CCPA-Related Case Foreshadows Five Issues," *Bloomberg Law*, February 10, 2020.
- Co-author, "'Data Brokers' Must Register With the California Attorney General by Tomorrow, January 31st," *Troutman Sanders*, January 30, 2020.
- Co-author, "Ill. Privacy Bill Is Not as Robust as Calif. Law," *Law360*, December 17, 2019.
- Co-author, "INSIGHT: Five Reasons to Comment on Draft CCPA Regulations," *Bloomberg Law*, October 22, 2019.
- Co-author, "Calif. Privacy Law Means New Approach to Vendor Contracts," *Law360*, September 27, 2019.
- Co-author, "Is Your Business in Need of a CCPA Intervention," *International Association of Privacy Professionals*, July 2019.
- Co-author, "Key Differences in Nev. and Calif. Data Privacy Laws," *Law360*, June 19, 2019.
- Co-author, "INSIGHT: So the CCPA Is Ambiguous—Now What?," *Bloomberg Law*, June 14, 2019.
- Co-author, "Five Lessons From Google's $57M Data Protection Fine," *Bloomberg Law*, February 7, 2019.
- Author, "Northern District of Georgia Rules in Equifax Data Breach Cases," *Consumer Financial Services Law Monitor*, January 30, 2019.
- Co-author, "Data Privacy: The Current Legal Landscape 2018 Reviewed," *Troutman Sanders News & Knowledge*, January 15, 2019.
- Author, "Iowa's New Year's Resolution: Making Consumer Security Freezes More Accessible and Enhancing Personal Information Security Breach Protection," *Consumer Financial Services Law Monitor*, December 31, 2018.
- Author, "One Breach, Two Breach, Three Breach! – A Closer Look at the Proposed Settlement for the *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*," *Consumer Financial Services Law Monitor*, November 21, 2018.

- Author, "Data Privacy: The Current Legal Landscape – September 2018," *Troutman Sanders News & Knowledge*, September 26, 2018.
- Co-author, "Clarity on Overlapping Background Check Laws in Calif.," *Law360*, August 22, 2018.
- Author, "Not Your Average Privacy Law—Vermont Enacts Nation's Most Expansive Data Broker Legislation," *Consumer Financial Services Law Monitor*, June 14, 2018.
- Author, "Hot Off the Press: NIST Releases Version 1.1 of Cybersecurity Framework," *Consumer Financial Services Law Monitor*, April 23, 2018.
- Author, "State AGs Have Bone to Pick With Proposed Federal Breach Notification Law," *Consumer Financial Services Law Monitor*, April 17, 2018.
- Co-author, "Talk About an Electric Shock – Power Company Fined $2.7M After Data Breach," *Consumer Financial Services Law Monitor*, March 22, 2018.
- Author, "Moving on to New Digital Identity (Authentication) Guidelines," *Consumer Financial Services Law Monitor*, February 12, 2018.

## Media Commentary

- Quoted, "Calif.'s Novel Privacy Moves May Dim Federal Law's Chances," *Law360*, October 5, 2022.
- Quoted, "Utah Sets New Floor In Joining Consumer Privacy Law Fray," *Law360*, March 29, 2022.
- Quoted, "2 State Cybersecurity, Data Privacy Laws Enacted," *GovInfoSecurity*, July 13, 2021.
- Interviewed, "Twitter Hack: Incident Response Lessons," *Security Media Group*, August 19, 2020.
- Interviewed, "CCPA Enforcement: What to Expect Now," *Data Breach Today*, July 8, 2020.
- Interviewed, "California Modifies Consumer Privacy Regulations - Again," *Bank Info Security*, March 24, 2020.
- Quoted, "Are Companies Adhering to CCPA Requirements?," *InfoRiskToday*, January 28, 2020.
- Quoted, "Will the U.S. Get a Federal Privacy Law?," *Data Breach Today*, December 27, 2019.

## Professional and Community Involvement

- Volunteer, Public Law Center
- Volunteer, Kids in Need of Defense

## Professional Experience

- Vice president /Assistant Division counsel, Black Knight Financial Services, 2015-2017
- Senior associate corporate counsel, CoreLogic, 2013-2015

## Bar Admissions

- California
- Texas

## Education

- Queen Mary University of London, LL.M., *with distinction*, 2013, banking and finance
- Stetson University College of Law, J.D., 2012, international law
- University of California, Los Angeles, B.A., 2009, English

## Certifications and Memberships

### Certifications

- Certified Information Privacy Professional/United States (CIPP/US)
- Certified Information Privacy Manager (CIPM)

## Languages

- Urdu

## Stephen C. Piepgrass

Partner
Richmond

stephen.piepgrass@troutman.com
D 804.697.1320


Stephen represents clients interacting with, and being investigated by, state attorneys general and other enforcement bodies, including the CFPB and FTC, as well as clients involved with litigation, particularly in heavily regulated industries.

**Areas of Focus:**

- Consumer Financial Services
- State Attorneys General
- Student Lending
- Regulatory Investigations, Strategy + Enforcement
- Marketing + Advertising

Stephen leads the firm's Regulatory Investigations, Strategy + Enforcement (RISE) Practice Group. He focuses his practice on enforcement actions, investigations, and litigation. Stephen primarily represents clients engaging with, or being investigated by, state attorneys general and other state or local governmental enforcement bodies, including the CFPB and FTC, as well as clients involved with litigation, with a particular focus on heavily regulated industries. He also has experience advising clients on data and privacy issues, including handling complex investigations into data incidents by state attorneys general other state and federal regulators. Additionally, Stephen provides strategic counsel to Troutman Pepper's Strategies clients who need assistance with public policy, advocacy, and government relations strategies.

Stephen also handles appellate cases and has appeared on brief in appeals to the U.S. Courts of Appeal for the Third and Fourth Circuits, the Supreme Court of Virginia, the Court of Appeals of Virginia, and amicus briefs to the United State Supreme Court, as well as various courts reviewing administrative decisions.

As a thought leader, Stephen provides ongoing analysis and commentary on regulatory developments and is a contributor to the firm's regulatory blog, Regulatory Oversight.

## Representative Matters

### State Attorneys General

- Representing a data and information services company in interactions with state attorneys general and other regulators.
- Representing a loan servicer in interactions with state attorneys general and other state governmental bodies.
- Representing an international home service contract provider in interactions with state attorneys general and other state governmental and quasi-governmental bodies.
- Represented an international pharmaceutical company with respect to issues related to knock-off products before state attorneys general.
- Interacted on behalf of client with national attorneys general associations, including the National Association of Attorneys General, the Republican Attorneys General Association, the Democratic Attorneys General Association, and the Conference of Western Attorneys General.
- Represented a group of alumnae who sued to prevent the closure of their college. Reached a successful mediated resolution resulting in an agreement to keep the college open under new leadership.

### Regulatory Privacy

- Represented a publicly traded company recognized as the world's leading cloud software provider, in a multistate investigation, as well as subsequent matters related to FTC, HHS, and SEC investigations, stemming from a data breach.
- Currently serving as counsel to a local government entity in an investigation related to a data breach incident.

### Local Government Law

- Serving as counsel to local government bodies on a wide range of issues, including government structure, boundary adjustments and disputes, annexations, consolidations, and disputes over utility service both inside and outside local boundaries.
- Advising clients dealing with zoning and land use issues.
- Representing local, state, and national campaigns, candidates, and government bodies dealing with election law issues, recounts, challenges to qualifications, and Voting Rights Act challenges.
- Defending local government bodies and individuals charged with civil and criminal malfeasance in office.

### Public Records

- Negotiated with local governments to preserve protections for companies engaged in public-private partnerships and development projects.
- Advised local government bodies on compliance with Freedom of Information Act and public meeting requirements.
- Represented a data company in dispute over use of public records in investigation and litigation by multistate group of state attorneys general and local governments.

- Represented a technology and data company in obtaining attorney general opinion on protections available under public records act for confidential information associated with data center development.
- Represented a biotechnology company working with locality in litigation over protection of trade secrets and public record laws.
- Represented a nonpartisan civic group in obtaining an injunction requiring Virginia election officials to make voter history lists available under Freedom of Information Act and the First Amendment for the purpose of encouraging voter participation.
- Advised a background screening company on use of public records in reports made available to customers.

## Related Practices and Industries

- Consumer Financial Services
- State Attorneys General
- Student Lending
- Better Business Bureau (BBB)
- Business Litigation
- Election Law + Government Ethics Compliance
- Election Law, Recount + Redistricting
- Enforcement Actions + Investigations
- Gaming
- Government + Regulatory
- Government + Regulatory Litigation
- Higher Education
- Incidents + Investigations
- Land Use + Zoning
- Litigation + Trial
- Labor + Employment Litigation + Dispute Resolution
- Public Records/FOIA

## Speaking Engagements

- Co-presenter, "The Interaction of Public Records and Business Under FOIA," Local Government Attorneys of Virginia Spring 2023 Conference, April 20-22, 2023.
- Co-presenter, "AG Investigations: Navigating Unwritten Rules, Protecting Confidentiality, and Managing Class Actions Risks," Strafford Publication, Inc., November 29, 2022.
- Speaker, "Hot Button Issues and Trends in State and Local Enforcement," Hispanic National Bar Association Annual Conference and Convention, September 22, 2020.
- Co-presenter, "Election Law 101: Gearing up for 2021 Redistricting and the Basics of Electoral Board Representation," Local Government Attorneys of Virginia, Spring 2020 Conference, May 29, 2020.

- Co-presenter, "Declaratory Judgment Actions: Remedies," Local Government Attorneys of Virginia Fall 2019 Conference, October 24-26, 2019.
- Speaker, "Consumer Financial Services Outlook 2019," Troutman Sanders Webinar, February 12, 2019.
- Speaker, "Protecting Confidentiality When Sharing Information With Regulators," December 12, 2017.
- Co-presenter, "When Third Parties Come Uninvited: Tortious Interference and Covenants Not to Compete," Virginia Bar Association, 7th Annual Advanced Business Litigation Institute, September 24, 2016.
- Panelist, "Telemarketing Sales Rule and Third Party Payment Processors," Webinar, Third Party Payment Processors Association (TPPPA), January 26, 2016.

## Publications

- Co-host, *Regulatory Oversight* Podcast.
- Co-author, "Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter," *Reuters* and *Westlaw Today*, October 16, 2023.
- Co-author, "Data Protection: One of These Incidents Is Not Like the Other," Reuters and Westlaw Today, August 24, 2023.
- Co-author, "Senate Proposal Opens the Door for More State Antitrust Lawsuits," *Troutman Pepper*, March 29, 2023.
- Co-author, "John Deere And Farmers Get Creative On 'Right To Repair'," *Law360*, March 2, 2023.
- Co-author, "2022 Regulatory Privacy Year in Review," *Troutman Pepper*, February 2, 2023.
- Co-author, "Preparing for an Era of Regulated Artificial Intelligence," *Law360*, January 25, 2023.
- Co-author, "State AGs Are Realizing Power of False Claims Statutes," *Law360*, December 8, 2022.
- Co-author, "Developing a Strategy for Settling Multistate AG Investigations," *Reuters*, November 10, 2022.
- Co-author, "Developing a Strategy for Settling Multistate AG Investigations," *Westlaw Today*, November 10, 2022.
- Co-author, "Tractor Hacking Newest Trick for Right to Repair," *Thomson Reuters Westlaw Today*, September 9, 2022.
- Co-author, "Regulatory Investigation Red Flags That Signal Significant Risk for Companies," *Reuters*, August 19, 2022.
- Co-author, "FOIA in the Supreme Court of Virginia: A Mid-Year Update," Local Government Attorneys *Bill of Particulars*, August 4, 2022.
- Co-author, "FTC Makes Good on Its Promise to Ramp up Right-to-Repair Enforcement," *Westlaw Today*, July 20, 2022.
- Co-author, "CFPB Deputy Director Takes Aim at 'Rent-a-Bank Schemes,'" *Troutman Pepper*, June 22, 2022.
- Co-author, "Preparing Companies for a New Day in Multistate AG Investigations," *Reuters*, June 13, 2022.

- Co-author, "Eight Republican AGs Express Concerns About Perceived Liberal Partisanship at NAAG," *Troutman Pepper*, May 26, 2022.
- Co-author, "Self-Regulation and Policymaking Guidance Regarding the Use of AI and ML," *RTInsights*, May 10, 2022.
- Co-author, "Ninth Circuit Provides Guidance on Web Scraping," *Troutman Pepper*, May 5, 2022.
- Co-author, "The Clash of Two Movements," *Thomson Reuters Westlaw Today*, April 22, 2022.
- Co-author, "State AG Cooperation on Opioids: A Model for Protecting Consumers," *Reuters*, February 17, 2022.
- Co-author, "State Coordination Will Continue to Regulate Use of Bitcoin," *Bitcoin Magazine*, January 21, 2022.
- Co-author, "Navient Settles with State AG Coalition Over Alleged Unfair, Deceptive, and Abusive Student Loan Origination and Servicing Practices," *Troutman Pepper*, January 20, 2022.
- Co-author, "States Attorneys General to Expand National Roles in 2022," *Bloomberg BNA*, December 29, 2021.
- Co-author, "California Passes CBD Law That Conflicts With FDA Guidance," *Regulatory Oversight Blog*, October 12, 2021.
- Co-author, "Technology as Protector: Challenges, Adaptations, and Best Practices for Remote Public Meetings During States of Emergency," *Ensuring an Informed Public: State Open Records and Meetings Laws*, American Bar Association, August 27, 2021.
- Co-author, "Regulators Likely to Focus on Hybrid Transactions and IoT Devices," *Intellectual Property & Technology Law Journal*, July-August 2021.
- Co-author, "It Could Be a Very Bitter Pill: US, Foreign, and State Antitrust Enforcement Agencies Launch Group to Change Traditional Analysis Applied to Pharmaceutical Mergers," *Troutman Pepper*, March 16, 2021.
- Co-author, "Republican AGs Likely to Challenge Biden on Multiple Fronts," *Law360*, March 3, 2021.
- Co-author, "State AGs Have a Decisive Role to Play in Election," *Law360*, October 30, 2020.
- Co-author, "How the State and Local Regulatory Landscape Is Expanding," *Law360*, October 16, 2020.
- Co-author, "The "New" Enforcers: How States and Localities Are Changing the Landscape of Regulatory Authority," *Troutman Pepper*, September 30, 2020.
- Co-author, "Decennial Redistricting in Virginia's Localities," Local Government Attorneys of Virginia, Spring 2020 Conference.
- Co-author, "As Virginia Enters Phase 2 of COVID-19 Recovery, Groups Must Reassess Public Meeting Obligations," *Richmond Times-Dispatch*, June 16, 2020.
- Co-author, "INSIGHT: State Attorneys General Can Deputize Attorneys to Fight Covid-19 Fraud," *Bloomberg Law*, May 21, 2020.
- Co-author, "Federal Judge Temporarily Halts Massachusetts' Sweeping COVID-19 Debt Collection Emergency Regulations," *Credit and Collection News,* May 7, 2020.
- Co-author, "Privacy Guidelines for COVID-19 Contact-Tracing App Makers," *Law360*, April 17, 2020.
- Co-author, "Public Meeting Requirements in the Age of COVID-19," *Law360*, April 14, 2020.

- Co-author, Regulatory Landscape, "2019 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Sanders*, February 24, 2020.
- Co-author, "Declaratory Judgment Actions: Remedies," Local Government Attorneys of Virginia Fall 2019 Conference, October 24, 2019.
- Co-author, "2018 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Sanders*, January 28, 2019.
- Co-author, "Expanding Authority: How the Virginia Attorney General Has Used the Virginia Consumer Protection Act to Augment Its Reach," *VBA Journal*, Fall 2018.
- Co-author, "Federal Inaction and State Activity: Student Loan Edition," Law360, August 1, 2018.
- Co-author, "Tussling Over Preemption: Emerging Battleground Between State Authorities and Student Loan Servicers," *Business Law Today*, May 15, 2018.
- Co-author, "Expert Analysis: A Potential Shift on Education Debt Discharge Standards," *Law360*, March 9, 2018.
- Co-author, "Takeaways From Dismissed Challenge to Trump's CFPB Pick," *Law360*, February 26, 2018.
- Co-author, "Dish Network Decision Underscores Importance of Compliance With Regulatory Settlements and Associated Litigation Risks," *National Association of Professional Background Screeners Journal*, January/February 2018.
- Co-author, "Appointment of CFPB Director Causes Rift Among State AGs," *Law360*, January 25, 2018.
- Co-author, "Annual Report: 2017 Consumer Financial Services Year in Review and a Look Ahead," January 10, 2018.
- Co-author, "Recent Developments in Virginia Election Law of Interest to Local Government Practitioners," *Journal of Local Government Law*, Spring 2016.

## Media Commentary

- Quoted, "23andMe Breach Compounded by Theft of Ethnicity Data," *Corporate Counsel*, November 7, 2023.
- Quoted, "Warranty Claims Spike, Target Tesla After FTC Action," *National Law Journal*, April 13, 2023.
- Quoted, "Will Noncompete Ban Pave Way for Similar Assault on NDAs?," *Law.com,* January 25, 2023.
- Interviewed, "Interview With Stephen C. Piepgrass, Partner, LGA Annual Sponsor Troutman Pepper Hamilton Sanders LLP," *Bill of Particulars*, October 2022.
- Quoted, "Happy to Be Regulated? Fallout From BlockFi Settlement Is a Matter of Speculation," *Cointelegraph*, February 21, 2022.
- Quoted, "As AG Takes Wheel at HHS, Biden Faces Rocky Legal Road," *Law360*, March 19, 2021.

## Professional and Community Involvement

- Member, Section of State and Local Government Law and State Attorneys General and Department of Justice Issues Committee, American Bar Association
- President (2014-2017), Board of Directors, Disability Law Center of Virginia Foundation

- Local Government Attorneys of Virginia
- Elder, Third Presbyterian Church, 2015-2018

## Rankings and Recognitions

- *Best Lawyers in America®:* Administrative / Regulatory Law (2024)
- Recognized in *The Legal 500 United States* for Government: State Attorneys General (2023)
- Rising Star, *Virginia Super Lawyers* (2010, 2013-2017)

## Professional Experience

- Summer law clerk, Hon. James H. Michael, Jr., U.S. District Court for the Western District of Virginia, 2003
- Communications director, U.S. Representative Mike Pence (IN-02), Washington, D.C., 2001-2002
- Deputy press secretary, U.S. Senator Sam Brownback (KS), Washington, D.C., 2000-2001
- Legislative correspondent, U.S. Representative Joseph R. Pitts (PA-16), Washington, D.C., 1999-2000

## Bar Admissions

- Virginia
- Pennsylvania

## Court Admissions

- U.S. District Court, Middle District of Pennsylvania
- U.S. District Court, Eastern District of Virginia
- U.S. District Court, Western District of Virginia
- U.S. Court of Appeals, Third Circuit
- U.S. Court of Appeals, Fourth Circuit
- Supreme Court of the United States

## Education

- University of Virginia School of Law, J.D., 2005, editor-in-chief, *Virginia Journal of International Law*
- Duke University, A.B., *cum laude*, 1999

## Ashley L. Taylor, Jr.

Partner
Richmond

ashley.taylor@troutman.com
D 804.697.1286
M 804.310.0934


Ashley is a nationally recognized and sought-after strategist and problem solver for clients facing bet-the-company government investigations, enforcement actions, and litigation. Drawing from his experience with industry-shaping, multistate investigations and litigation, he provides clear-cut advice for his clients' toughest challenges.

**Areas of Focus:**

- State Attorneys General
- Enforcement Actions + Investigations
- Consumer Financial Services
- Regulatory Investigations, Strategy + Enforcement
- Marketing + Advertising

Ashley is co-leader of the firm's nationally ranked State Attorneys General practice, vice chair of the firm, and a partner in its Regulatory Investigations, Strategy + Enforcement (RISE) Practice Group. He helps his clients navigate the complexities involved with multistate attorneys general investigations and enforcement actions, federal agency actions, and accompanying litigation.

Ashley's clients benefit from his experience as a former deputy attorney general and the insights gained from handling high stakes matters before every state attorney general (AG) in U.S. as well as the federal agencies that regulate his clients' businesses. While he is experienced across a wide range of heavily regulated sectors, Ashley offers exceptional experience in the financial services industry, including issues involving the Federal Credit Reporting Act (FCRA), the Fair Debt Collections Practices Act (FDCPA), State Consumer Protection laws, and before agencies such as the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC).

The outcomes Ashley achieves on behalf of his clients are due, in part, to his knowledge of the regulatory enforcement priorities of each state AG and their approaches to enforcement actions and investigations. His long-standing relationships with personnel at all levels in state AG offices throughout the U.S., combined with his ability to apply effective risk management strategies in the face of multiple government actions and litigations, enables him to efficiently resolve his clients' largest and most mission-critical challenges. As government scrutiny continues to intensify across many consumer facing industries, Ashley informs his

clients of the latest regulatory trends and emerging issues through comprehensive counseling and frequent thought leadership.

Ashley is deeply involved with attorneys general organizations, including the National Association of Attorneys General (NAAG). He founded, and co-chairs the American Bar Association committee on state attorneys general matters. He previously served as a commissioner on the U.S. Commission on Civil Rights, appointed by President Bush from 2004 to 2010.

As a thought leader, Ashley provides ongoing analysis and commentary on regulatory developments. He often writes about issues in the state and federal regulatory landscape, and his work can be found on the firm's Regulatory Oversight blog.

## Representative Matters

### Multistate State Attorneys General Investigations

- Selected to serve as an expert witness in a dispute related to a multistate attorneys general investigation.
- Successfully settled more than a dozen False Claims Act investigations against an international data and analytics company.
- Successfully resolved a 40-state investigation of a national automobile manufacturer relating to alleged manufacturing defects
- Successfully resolved a 44-state investigation of a data broker relating to a data breach.
- Negotiated settlement of a 33-state investigation of a leading pharmacy benefit manager involving "undisclosed" rebates.
- Drafted and effectively advocated for advancement of National Association of Attorneys General model legislation on behalf of a national trade association.
- Successfully resolved a multistate investigation of a national pharmaceutical company involving off-label marketing.

### Single State Investigations

- Representing a finance company in an investigation by the Massachusetts Attorney General relating to alleged violations of the state's False Claims Act and Consumer Protection Act stemming from the company's auto loan origination, collection, and securitization practices.
- Representing a tenant screening company in an investigation by the California Attorney General in what is likely the first investigation by that office relating to a newly implemented section of the California Consumer Credit Reporting Agencies Act relating to the prevention of housing and tenant industries from using COVID-19 rental debt as a negative factor for the purposes of evaluating a prospective housing application.
- Representing the tenant screening company in an investigation by the Massachusetts Attorney General in connection with screening and background check services.

### Litigation

- Representing a publicly traded technology company in a multidistrict litigation arising out of an alleged data breach.

- Representing a national company in litigation grounded in consumer protection brought by the District of Columbia Attorney General.
- Representing a government contractor in a multijurisdictional ownership dispute.
- Represented a national leader in short-term credit solutions in the first Virginia Attorney General investigation following the comprehensive overhaul of nonbank lending legislation.
- Successfully defended litigation brought by the AG relating to the company's compliance with the Fairness in Lending Act and Consumer Protection Act.

### Compliance and Internal Investigations

- Representing the majority shareholder of a holding company for several debt collection agencies in connection with the proactive mitigation of potential regulatory risks in more than 35 states and territories.
- Assisted client concerning a nationwide evaluation of disclosure requirements and developed an outreach and engagement strategy to avert possible adverse regulatory action.
- Representing a publicly traded utility in an internal investigation relating to potential employee misconduct
- Representing a municipality in an internal investigation involving the death of a minor who had been placed in the care of the municipality.

***Representative matters may include engagements before joining Troutman Pepper.***

## Related Practices and Industries

- State Attorneys General
- Enforcement Actions + Investigations
- Consumer Financial Services
- Better Business Bureau (BBB)
- Consumer Financial Protection Bureau (CFPB)
- Consumer Products
- Election Law, Recount + Redistricting
- Fair Credit Reporting Act (FCRA)
- Federal Trade Commission (FTC)
- Gaming
- Government + Regulatory
- Government + Regulatory Litigation
- Higher Education
- Litigation + Trial
- Payments + Financial Technology
- Tobacco + Nicotine
- Tribal Lending

- Incidents + Investigations

## Speaking Engagements

- Speaker, "Greater Philadelphia In-House Counsel Conference 2023," Association of Corporate Counsel, April 20, 2023.
- Moderator, "Navigating a Data Breach From Start to Finish," ABA 2023 Corporate Counsel CLE Seminar, February 18, 2023.
- Speaker, "Corporate Counsel Institute," State Bar of Georgia, December 16, 2022.
- Panelist, "State Law and Enforcement Trends," MBA Legal Issues Conference, May 24, 2022.
- Panelist, "The Coordination Rodeo: Options for Lassoing Parallel Proceedings," ABA National Institute on Class Actions, April 12, 2022.
- Panelist, "Data Breaches and Their Impact on Litigation Policy," IMS Insights Live Panel Event, November 10, 2021.
- Panelist, "Compliance Frameworks: Making Them Work for the Greater Good," Uniting Women in Cyber Conference, The Cyber Guild, October 5, 2021.
- Speaker, "Recent Developments in Data Privacy Legislation and Regulation," Troutman Pepper, May 5, 2021.
- Speaker, "Operationalizing the Virginia Consumer Data Protection Act: Leveraging Lessons From the CCPA," Troutman Pepper, April 15, 2021.
- Presenter, "Strategies to Prepare for Six Potential Target Areas of CCPA Enforcement by the CA Attorney General," Troutman Pepper Webinar, August 19, 2020.
- Presenter, "COVID-19: CCPA and Regulatory and Governmental Litigation Update," Troutman Sanders Webinar, May 7, 2020.
- Panelist, "Consumer Debtor Protections & Rights for Low-Income Americans During the COVID-19 Pandemic," American Bar Association Webinar, April 14, 2020.
- Speaker, "Quick Answers to Critical COVID-19 Compliance Questions for Financial Services Companies," Troutman Sanders Webinar, March 31, 2020.
- Speaker, "TCPA Update," Credit and Collection News Annual Conference, Lake Tahoe, CA, April 11-12, 2018.
- Speaker, "Abusive Car Loan and Sale Practices: Scope and Potential Remedies to Strengthen Consumer Protections," American Bar Association Webinar, March 22, 2018.
- Speaker, "An Inside View: Working With Your Attorney General," American Bar Association Webinar, February 13, 2018.
- Speaker, "Enforcement Agencies Confront Class Actions," American Bar Association Webinar, December 5, 2017.
- Speaker, "Defending Consumer Protection Actions on Multiple Fronts: Coordinating Joint CFPB and State AG Investigations and Settlements," American Bar Association Webinar, November 27, 2017.
- Speaker, "The New Look of Financial Regulation," Virginia Bar Association Administrative Law Conference, Richmond, VA, November 9, 2017.

- Speaker, "Working With Your Attorney General," Credit and Collection News Annual Creditor Grantor Summit, Washington, D.C., August 14-16, 2017.
- Presenter, "The CHOICE Act Passed the House: Now What? An Update on Financial Industry Regulation Under the Trump Administration," Troutman Sanders Consumer Financial Services Webinar Series, June 29, 2017.
- Panelist, "Legal and Regulatory Update," Third Party Payment Processors Association Annual Conference, Washington, D.C., May 19, 2017.
- Moderator, "Squaring the Circle: Finding Creative Solutions to Regulatory Challenges," Consero Financial Services and Insurance Litigation Forum, Coral Gables, FL, April 3, 2017.
- Panelist, "The Future of the CFPB: New Agency Structure, New Enforcement Tactics and Joint Enforcement Efforts," National Association of Professional Background Screeners Mid-Year Legislative & Regulatory Conference, Washington, D.C., March 20, 2017.
- Panelist, "How Will the Trump Administration Impact the Banking and Financial Services Industry?," Troutman Sanders Consumer Financial Services Webinar Series, December 14, 2016.
- Panelist, "Legal and Regulatory Update," Third Party Payment Processors Association Executive Summit, Phoenix, AZ, November 10, 2016.
- Speaker, "Working With Your Attorney General," Credit and Collections News Annual Credit Grantor Consortium, Washington, D.C., August 16, 2016.
- Speaker, "State Regulatory & Enforcement Update," Consumer Relations Annual Consortium, Washington, D.C., August 5, 2016.
- Moderator, "Finding Creative Regulatory Solutions," Consero Financial Services & Insurance Litigation Forum, Coral Gables, FL, April 19, 2016.
- Panelist, "Regulatory Enforcement – A View From the Inside," National Association of Professional Background Screeners Mid-Year Legislative & Regulatory Conference, Washington, D.C., April 5, 2016.
- Panelist, "Working With Your Attorney General," Credit and Collection News Annual Conference, Amelia Island, FL, March 31, 2016.
- Moderator, "Adapting to Changing Regulatory, Legislative & Enforcement Activities and Breach Notification Requirements," American Conference Institute 18th Advanced Global Legal & Compliance Forum on Cyber Security and Data Privacy & Protection, Washington, D.C., January 28, 2016.
- Panelist, "State Attorneys General: Emerging Leaders in Consumer-Related Issues," Corporate Counsel Institute, Atlanta, GA, December 11, 2015.
- Panelist, "Emerging Enforcement Trends and Related Privacy Issues," Third Party Payment Processor Association (TPPPA) Member Executive Leadership Summit and Retreat, Phoenix, AZ, November 18, 2015.
- Moderator, "Emerging Regulatory, Legislative, and Enforcement Activities and Breach Notification Requirements," American Conference Institute (ACI), 17th Installment, Cyber Security & Data Privacy and Protection, Houston, TX, October 5-6, 2015.
- Conference Co-chair & Panel moderator, "Unique Regulatory and Enforcement Insights by State Attorneys General and Consumer Protection Agencies on Emerging Privacy Initiatives, Settlement and Enforcement Trends, Security Breach Notification Requirements, and More," American Conference Institute (ACI), 15th Installment, Global Legal & Compliance Forum on Cyber Security & Data Privacy and Protection, Washington, D.C., January 15-16, 2015.

- Speaker, "The Latest Collection Hot Topics," Credit and Collection News, 9th Annual Credit Grantor Consortium, Washington, D.C., August 19, 2014.
- Moderator, "Keeping Up With the Regulators," Consero Financial Services & Insurance Litigation Forum, Miami, FL, May 19, 2014.
- Moderator, "CFPB Update," Credit and Collection News, 9th Annual Credit Grantor Consortium, Washington, D.C., August 20, 2014.
- Speaker, "The Class Action Fairness Act and State Attorney General Enforcement Actions: Does the Supreme Court's Ruling Open a New Door for the States?" American Bar Association, Annual Meeting, Boston, MA, August 9 , 2014.
- Moderator, "Deputy State Attorneys General Update," 9th Annual Credit and Collection News Conference, Naples, FL, April 2, 2014.
- Moderator, "Privacy in the Digital Age: Is There Even a Barn Door Left to Close?," ABA Midyear Meeting, Chicago, IL, February 6, 2014.
- Presenter, "CFPB, FTC, State Regulators and Compliance," Credit and Collection News Seminar, New York City, NY, September 17-18, 2013; Los Angeles, CA, November 12-13, 2013; Atlanta, GA, February 18-19, 2014.
- Conference Co-chair and Moderator, "Unique Regulatory and Enforcement Insights by State Attorneys General and Consumer Protection Agencies on Emerging Privacy Initiatives, Settlement and Enforcement Trends, Security Breach Notification Requirements, and More," ACI Privacy & Security of Consumer and Employee Information, Washington, D.C., January 16-17.
- Speaker, "Chat With the AG's on State Issues," Credit and Collection News 8th Annual Credit Grantor Consortium, Washington, D.C., August 13, 2013.
- Panelist, "CFPB & State Attorneys General Compliance," American Bar Association Annual Meeting, San Francisco, CA, August 10, 2013.
- Presenter, "Promotions in Rhode Island & New York," The Global Regulatory Year in Review, Tobacco Merchants Association's 98th Annual Meeting & Conference, Williamsburg, VA, Thursday, May 16, 2013.
- "Working With Your State Attorney General," 8th Annual Credit and Collection News Conference, Half Moon Bay, CA, April 3, 2013.
- "State Attorneys General: Chief Deputy Attorneys General Panel," 8th Annual Credit and Collection News Conference, Half Moon Bay, CA, April 2, 2013.
- "State Attorneys General and Consumer Protection Agencies: Emerging State Privacy Initiatives, Settlement and Enforcement Trends and Security Breach Notification Requirements," American Conference Institute's 13th Annual Legal and Compliance Forum on Privacy and Security of Consumer and Employee Information, Washington, D.C., February 5, 2013.
- "Top 8 Rules for Dealing With State Insurance Regulators," presented to in-house legal department of *Fortune 500* company, Richmond, VA, January 29, 2013.
- "New Voter Registration Laws: Fighting Voter Fraud or Suppressing the Vote?," ABA Section of State and Local Government, Criminal Justice Section, and the Center for Professional Development, Webinar and Teleconference, November 5, 2012.
- "Working With Your Attorneys General," Credit and Collection News 7th Annual Credit Grantor Consortium, Washington, D.C., August 8, 2012.

- "New Voter Registration Laws: Fighting Voter Fraud or Suppressing the Vote?," ABA State & Local Government Law Section, Annual Meeting, Showcase Panel Presentation, Chicago, IL, August 5, 2012.
- "Attorneys General and Consumer Protection Agencies Speak Out on Emerging State Privacy Initiatives, Settlement and Enforcement Trends and Security Breach Notice Requirements," American Conference Institute's 12th National Legal and Compliance Forum on Privacy and Security of Consumer and Employee Information, San Francisco, CA, July 30, 2012.
- "The Ten Most Significant Attorney General Investigations/Settlements Involving Technology," The University of Dayton School of Law's Twentieth Annual Seminar on Significant Developments in Computer and Cyberspace Law, Dayton, OH, June 11, 2010.
- "Emerging State Enforcement Activities and Investigations and the Growing Authority of the State Attorneys General," American Conference Institute's National Advanced Forum on Litigation and Enforcement Preparedness for Data Privacy & Information Security, Dallas, TX, June 2010.
- "Federalism - The Ever Evolving Relationship Between the Federal and State Governments," American Bar Association State and Local Government Annual Meeting, San Francisco, CA, August 2010.
- "Working With AGs to Maneuver Your Way Through the Investigation Process," American Conference Institute's 9th Annual Conference on Consumer Finance Class Actions & Litigation, January 2010.
- "State Attorneys General: Responding to Multi-State Regulatory Compliance Investigations," American Bar Association Panel Seminar, July 2009.
- "From Cradle to Grave: Regulatory Investigations Which Beget Complex Business Litigation," Washington Metropolitan (WMACCA) Chapter of Association of Corporate Counsel, May 2009.
- "Multi-State Investigations and Suits: How to Address the Expanding Authority and Ambition of State Attorneys General," Washington Legal Foundation's Web Seminar Series, March 2009.
- "State Attorneys Investigation," American Legislative Exchange Council, November 2008.

### Consumer Financial Protection Bureau

- Speaker, "Understanding the CFPB and State Attorneys General Regulatory Issues Relating to Debt Collection," Credit and Collection News Webinar, March 7, 2013.
- "The Consumer Financial Protection Bureau and State Attorneys General Compliance," Credit and Collection News Webinar, November 13, 2012.
- "The Consumer Financial Protection Bureau (CFPB): The New World Order – Enforcement by State Attorneys General and the Consumer Financial Protection Bureau," American Conference Institute, September 20, 2011.
- "State Attorneys General: Responding Successfully to Regulatory Compliance Matters and Investigations," Credit and Collection News Conference – Collection Agency Consortium, August 18, 2011.

## Publications

- Co-host, *Regulatory Oversight* Podcast.
- Co-author, "State Attorney General Actions: How Outside Counsel for AGs Changes the Game," *Westlaw Today*, June 30, 2023.
- Co-author, "Five Ways to Effectively Navigate Litigation With State Attorneys General," *Westlaw Today*, April 12, 2023.

- Co-author, "State AGs May Put Investors on the Hook for Co. Bad Acts," *Law360*, February 22, 2023.
- Co-author, "State Attorney General Actions: Strategies for Venue and Settlement Differ From Typical Litigation," *Reuters*, February 16, 2023.
- Co-author, "How Approaches in State Attorney General Actions Differ From Typical Litigation," *Reuters*, February 8, 2023.
- Co-author, "2022 Regulatory Privacy Year in Review," *Troutman Pepper*, February 2, 2023.
- Co-author, "State AGs Are Realizing Power of False Claims Statutes," *Law360*, December 8, 2022.
- Co-author, "Developing a Strategy for Settling Multistate AG Investigations," *Reuters*, November 10, 2022.
- Co-author, "Developing a Strategy for Settling Multistate AG Investigations," *Westlaw Today*, November 10, 2022.
- Co-author, "Regulatory Investigation Red Flags That Signal Significant Risk for Companies," *Reuters*, August 19, 2022.
- Co-author, "Focusing on the Primary Purpose: Protecting the Attorney–Client Privilege and Work Product Doctrine in Incident Response," *Cyber Security: A Peer-Reviewed Journal*, July 11, 2022.
- Co-author, "CFPB Deputy Director Takes Aim at 'Rent-a-Bank Schemes,'" *Troutman Pepper*, June 22, 2022.
- Co-author, "Preparing Companies for a New Day in Multistate AG Investigations," *Reuters*, June 13, 2022.
- Co-author, "Eight Republican AGs Express Concerns About Perceived Liberal Partisanship at NAAG," *Troutman Pepper*, May 26, 2022.
- Co-author, "Federal Contractors on Notice After DOJ Announces First Civil Cyber Fraud Initiative Settlement," *Troutman Pepper*, April 21, 2022.
- Co-author, "Your Company May Be a Likely Target of State Attorneys General. You May Not See It Coming," *Corporate Compliance Insights*, February 15, 2022.
- Co-author, "Navient Settles with State AG Coalition Over Alleged Unfair, Deceptive, and Abusive Student Loan Origination and Servicing Practices," *Troutman Pepper*, January 20, 2022.
- Co-author, "States Attorneys General to Expand National Roles in 2022," *Bloomberg BNA*, December 29, 2021.
- Co-author, "The Virginia Consumer Data Protection Act, the Colorado Privacy Act, and the Draft Connecticut Privacy Legislation: An Overview and Practical Guide," *The National Law Review*, November 2021.
- Co-author, "Thirty State Attorney General Offices Are up for Grabs," *Reuters*, October 13, 2021.
- Co-author, "New UK Standards for Children's Digital Services Take Effect — Provides Framework for New US Law," *Troutman Pepper*, September 23, 2021.
- Co-author, "Movement on All Sides Toward Broader Data Privacy and Security Oversight by FTC," *Troutman Pepper*, September 20, 2021.
- Co-author, "Top Takeaways From a Year of CCPA Enforcement," *Bloomberg Law*, August 6, 2021.
- Co-author, "Litigation and Enforcement: Virginia Consumer Data Protection Act Series (Part Five)," *Troutman Pepper*, April 1, 2021.

- Co-author, "Data Processing Obligations: Virginia Consumer Data Protection Act Series (Part Four)," *Troutman Pepper*, March 25, 2021.
- Co-author, "Notice and Disclosure Obligations: Virginia Consumer Data Protection Act Series (Part Three)," *Troutman Pepper*, March 18, 2021.
- Co-author, "Consumer Rights: Virginia Consumer Data Protection Act Series (Part Two)," *Troutman Pepper*, March 11, 2021.
- Co-author, "Introduction and Overview: Virginia Consumer Data Protection Act Series (Part One)," *Troutman Pepper*, March 4, 2021.
- Co-author, *Consumer Finance Law: Understanding Financial Services Regulations*, American Bar Association, February 25, 2021.
- Co-author, "State AGs' 2020 Actions Offer Hints at 2021 Priorities," *Law360*, January 12, 2021.
- Co-author, "State AGs Have a Decisive Role to Play in Election," *Law360*, October 30, 2020.
- Co-author, "State Challenges to U.S. Postal Service Leading Up to 2020 Election," *Troutman Pepper*, September 30, 2020.
- Co-author, "The Coming Tsunami: Anticipated Regulatory and Enforcement Trends in the Wake of COVID-19 and the Unique Role of State Attorneys General," *Business Law Today*, June 10, 2020.
- Co-author, "Mortgage Industry Should Prepare for Forbearance Scrutiny," *Law360,* June 9, 2020.
- Co-author, "INSIGHT: State Attorneys General Can Deputize Attorneys to Fight Covid-19 Fraud," *Bloomberg Law*, May 21, 2020.
- Co-author, "Federal Judge Temporarily Halts Massachusetts' Sweeping COVID-19 Debt Collection Emergency Regulations," *Credit and Collection News,* May 7, 2020.
- Co-author, "Privacy Guidelines for COVID-19 Contact-Tracing App Makers," *Law360*, April 17, 2020.
- Co-author, "Public Meeting Requirements in the Age of COVID-19," *Law360*, April 14, 2020.
- Co-author, "2019 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Sanders*, February 24, 2020.
- Co-author, "Expanding Authority: How the Virginia Attorney General Has Used the Virginia Consumer Protection Act to Augment Its Reach," *VBA Journal*, Fall 2018.
- Author, "How Regulatory Power Is Moving to the States," *Law360*, March 20, 2018.
- Co-author, "Dish Network Decision Underscores Importance of Compliance With Regulatory Settlements and Associated Litigation Risks," *National Association of Professional Background Screeners Journal*, January/February 2018.
- Co-author, "Federal Deregulation Opens the Door for State-Level Threats to Auto Finance," *Business Law Today*, January 16, 2018.
- Co-author, "Annual Report: 2017 Consumer Financial Services Year in Review and a Look Ahead," January 10, 2018.
- Co-author, "When Gov't Enforcement Actions And Class Actions Collide," *Law360*, December 7, 2017.
- Co-author, "DOJ Brief Opposing CFPB Brings More Uncertainty," *Law360*, March 19, 2017.
- Co-author , "Expect Greater FTC Scrutiny in Wake of Schrems," *Law360,* October 27, 2015.

- "Walking a Tightr ope: State Attorney General Enforcement Authority and Private Counsel Contingency Fee Arrangements," *American Bar Association State and Local Government Law News*, Vol. 36, No. 3, Spring 2013.
- "The Removability of Consumer Protection Lawsuits Filed by State Attorneys General," *American Bar Association State & Local Law News*, Vol. 35, No. 3, Spring 2012.
- Co-author , "State Attorneys General: The Robust Use of Previously Ignored States Powers,"*The Urban Lawyer, The National Journal on State and Local Government Law*, Summer 2008.
- "ChoicePoint Official: Experienced Counsel Key for Multi-State AG Probes," *The Bureau of National Affairs, Inc.,* July 2007.
- Co-author , "Cases Involving Government Agencies Present Unique Discovery Issues," *Atlantic Coast In-House Counsel,* July 2005.
- "Effectively Responding When the State Attorneys General Are Arrayed Against Your Company," *Atlantic Coast In-House,* March 2004.

### Consumer Financial Protection Bureau

- "The Consumer Financial Protection Bureau and the State Attorneys General: A Force Multiplier in Consumer Protection Matters," *Bloomberg Law Reports*, May 25, 2011.

## Media Commentary

- Quoted, "Litigators Who Lead Firm-Wide Practices Balance Subject Matter Mastery With 'the Soft Skills'," *Law.com*, October 5, 2023.
- Interviewed, "How I Made It to Law Firm Leadership: 'Surround Yourself With People Smarter Than You and Be Accountable,' Says Ashley L. Taylor Jr. of Troutman Pepper," *Law.com*, March 2, 2023.
- Interviewed, "Want to Know State AGs' Priorities? Just Look at Their Settlement Agreements, Says Troutman Pepper's Ashley Taylor," *Law.com/The AmLaw Litigation Daily*, November 16, 2021.
- Quoted, "Consumer Bureau Chief Confirmed in Close Senate Vote," *The New York Times*, September 30, 2021.
- Quoted, "Va. Set to Become 2nd State With Consumer Data Protection Law," *Virginia Business*, March 1, 2021.
- Quoted, "GOP Readies Counterpunch if Biden Removes CFPB Chief," *American Banker*, November 23, 2020.
- Quoted, "CFPB Under Biden Will Likely Get New Director, New Direction," *Compliance Week*, November 9, 2020.
- Quoted, "Trump Unhappy With Legal Team's Lack of Major Impact on Election Count," *CNN*, November 6, 2020.
- Quoted, "Flowers Case Shows How AGs Are Stepping Into the Spotlight," *Law360*, September 13, 2020.
- Interviewed, "Regulatory Takings and Executive Power to Seize Property," Troutman Sanders and Pepper Hamilton COVID-19 Litigation Podcast Series, COVID-19 Resource Center, April 25, 2020.
- Quoted, "States Prepare to Step in If CFPB Enforcement Slows in 2018," *Bloomberg BNA*, December 13, 2017.

- Quoted, "$280M Dish TCPA Penalty May Make Settling More Attractive," *Law360*, June 8, 2017.
- Quoted, "Foxfield Lawsuit: Plaintiffs Say There's No Finish Line in Sight," *c-ville*, January 25, 2017.
- Quoted, "States Flexing Enforcement Muscle on Prospect of CFPB Pullback," *Bloomberg BNA*, September 6, 2017.
- Quoted, "Would Weakening Regulators' Edge in Court Backfire on Banks?," *American Banker*, February 21, 2017.
- Quoted, "CFPB Clearing Decks With Slew of Lawsuits as Cordray Battle Looms," *American Banker*, January 23, 2017.
- Quoted, "U.S. States Likely to Coordinate Reviews of Time Warner Cable/Comcast With DOJ, Attorneys Say," *Policy and Regulatory Report*, March 24, 2014.
- "Troutman Sanders' Ashley Taylor on the Rise of the State Attorneys General," *Corporate Crime Reporter*, July 2009.

## Professional and Community Involvement

- Fellow, American Bar Association
- Member, St. Catherine's School Board of Governors; chair, Diversity, Equity and Inclusion Committee
- Board member, The Richmond Forum
- Founding chair, State Attorneys General and Department of Justice Issues Committee, Section of State and Local Government Law, American Bar Association, 2013-present
- Former and current Board member, St. Christopher's School, 2009-2015, 2018-2021
- Member, Virginia Bar Association's Committee on Federal Judgeships, Eastern District
- Member, Commission on Virginia Courts in the 21st Century, appointed by Chief Justice Hassell
- Former member, Executive Counsel, American Bar Association, Young Lawyers Division
- Former member, Executive Committee, Virginia Bar Association, Young Lawyers Division
- Former director, Virginia Military Institute Athletic Association (The Keydet Club)

## Rankings and Recognitions

- Recognized in *The Legal 500 United States* for Government: State Attorneys General (2023)
- *Virginia Lawyers Weekly*: Go To Lawyers – Business Litigation (2023)
- *Best Lawyers in America*®: Commercial Litigation (2013-2024), Corporate Law (2011-2024), Privacy and Data Security Law (2024)
- *Super Lawyers:* Virginia (2021)
- *Chambers USA*: State Attorneys General, USA Nationwide (2015-2023)
- Recognized in *The Legal 500 United States* for Firms to Watch editorial for Government: Government relations (2022)
- *Savoy Magazine*: "Most Influential Black Lawyers" (2018)
- *Law and Politics*: "Super Lawyer" in Civil Litigation Defense and Consumer Law (2006-2012)

- *Virginia Business Magazine*: "Legal Elite" in Legislative and Regulatory (2004, 2010)
- *Virginia Business Magazine*: "Legal Elite" in Civil Litigation (2005, 2007, 2009)
- *National Law Journal*: "50 Most Influential Minority Lawyers in America" (2008)
- *Style Weekly*: "Top 40 Under 40" (2007)
- Named by the American Bar Association State and Local Government Section as the "Up and Comer" of the Year (1999)

## Professional Experience

- Commissioner, United States Commission on Civil Rights, Appointed by President George W. Bush (December 2004–2010)
- Deputy Virginia attorney general (1998–2001)

## Bar Admissions

- Virginia

## Court Admissions

- Supreme Court of the United States
- U.S. Court of Appeals, Fourth Circuit
- U.S. District Court, Eastern District of Virginia
- Supreme Court of Virginia

## Education

- Washington and Lee University School of Law, J.D., 1993
- Virginia Military Institute, B.A., 1990

## Clerkships

- United States District Court, 1993 - 1995

# Samuel E. "Gene" Fishel

Counsel
Richmond

gene.fishel@troutman.com
D 804.697.1263


Gene is a former regulator with two decades of experience who has overseen state cybersecurity regulation enforcement, led national, multistate attorneys general privacy investigations, and prosecuted computer crimes at the state and federal levels. He has served at the forefront of state attorney general and federal enforcement, and utilizes this experience to proficiently represent client interests.

**Areas of Focus:**

- State Attorneys General
- Government + Regulatory
- Privacy + Cyber

Gene is a member of the firm's Regulatory Investigations, Strategy + Enforcement (RISE) practice, based in the Richmond office. He brings extensive regulatory experience, having most recently served as senior assistant attorney general and chief of the Computer Crime Section in the Office of the Attorney General of Virginia, and as special assistant U.S. attorney in the Eastern District of Virginia for 20 years.

As a regulator, Gene has reviewed thousands of database breach incidents and investigated hundreds of cybersecurity, privacy, and consumer protection violations, including as part of multistate attorneys general teams. He has been a pillar in the charge for sweeping reforms to privacy and computer crime laws, having drafted and shepherded dozens of successful bills involving database breach notification, electronic records, identity theft, computer trespass, and child exploitation statutes, among others. In his supervisory capacities, he led the professional development of attorneys and computer forensic examiners, overseeing more than 1,000 prosecutions and computer forensic investigations for complex criminal cases in Virginia.

With an exemplary understanding of applying existing law to evolving cybersecurity and privacy problems, he guides clients navigating such issues and advises them at every stage of a matter.

## Representative Matters

- Reviewed more than 4000 database breach incidents and filed more than three dozen privacy enforcement actions resulting in settlements.

- Participated in more than 100 multistate, attorneys general privacy and consumer protection investigations as a member of the National Association of Attorneys General Privacy Working Group.
- Handled more than 400 state and federal prosecutions related to complex computer crimes, including the Virginia Computer Crimes Act, identity theft, child exploitation, and the federal Computer Fraud and Abuse Act.
- Prosecuted the first, felony case in the U.S. for illicit spamming in 2004.

***Representative matters may include engagements before joining Troutman Pepper.***

## Related Practices and Industries

- Regulatory Investigations, Strategy + Enforcement
- Privacy + Cyber
- Incidents + Investigations

## Speaking Engagements

- Speaker, "Benefits of Legal and CISOs Uniting in a Post-Uber and Twitter World," InfoSec World, September 26, 2023.
- Speaker, "Regulatory Approaches to AI," State Bar of Michigan IT Law Section's Annual Summit, September 21, 2023.
- Panelist, "US Regulatory Update: View from the States," NetDiligence Cyber Risk Summit, Philadelphia, PA, 2022, 2023.
- Panelist, "Federal and State Regulators Panel," American Conference Institute's Cyber Risk and Liability Conferences, Consumer Finance Conferences, and Data Risk Insurance Conferences, Chicago, Miami, New York, San Francisco, Washington, D.C., 2011-2018.
- Panelist, "A Focus on Settlement of Cybersecurity Class Actions and Regulatory Investigations," NetDiligence Cyber Risk and Privacy Liability Forum, Santa Monica, CA, 2016, 2017.
- Keynote speaker, "Legal Issues Involving Electronic Evidence," National Social Media in Law Enforcement (SMILE) Conference, Alexandria, VA, 2016.
- Keynote speaker, "State Level Computer Security Issues and Enforcement," RVASEC Mid-Atlantic Publications
- Co-author, "Your Organization Has Suffered a Data Incident: Now Here Are the Regulators It Will Likely Encounter," *Reuters* and *Westlaw Today*, October 16, 2023.
- Co-author, "Data Protection: One of These Incidents Is Not Like the Other," Reuters and Westlaw Today, August 24, 2023.

## Professional and Community Involvement

- Adjunct professor, University of Richmond School of Law, 2022-present
- Former ex-officio member, Virginia State Bar Criminal Law Section Board of Governors, 2011-present (chair, 2020-2021)

- Former member, VA Department of Education's Digital Citizenship, Internet Safety, and Media Literacy Council, 2019-2023
- Former member, Governor's Secure Commonwealth of Virginia Cyber Security Subpanel, 2016-2023
- Former staff, Virginia Cyber Security Commission, 2014-2016
- Former member, Joint Committee on Technology and Science Advisory Committee, Virginia General Assembly, 2013
- Former member, Governor's Office of Substance Abuse Prevention Advisory Committee, 2010-2011
- Former member, Joint Committee on Technology and Science Advisory Committee, Virginia General Assembly, 2010
- Former staff, Governor's Data Breach Notification Advisory Committee, 2007
- Former member, Joint Committee on Technology and Science Advisory Committee, Virginia General Assembly, 2007
- Former member, National White Collar Crime Center Cybercrime Advisory Committee, 2003-2005

## Professional Experience

- Senior assistant attorney general, chief – Computer Crime Section, Virginia Attorney General's Office, 2007-2023
- Special assistant U.S. attorney, Eastern District of Virginia, 2003-2023
- Special assistant U.S. attorney, Western District of Virginia, 2004-2017
- Assistant attorney general, Computer Crime Section, Virgiia Attorney General's Office, 2003-2007
- Law clerk, Second Judicial Circuit of Virginia, 2002-2003

## Bar Admissions

- Virginia

## Court Admissions

- Supreme Court of Virginia
- U.S. District Court, Eastern District of Virginia
- U.S. District Court, Western District of Virginia
- U.S. Court of Appeals, Fourth Circuit

## Education

- Wake Forest University School of Law, J.D., 2002
- James Madison University, B.A., *magna cum laude*, 1999

## Karla Ballesteros

Associate
Orange County

karla.ballesteros@troutman.com
D 949.622.2415


**Areas of Focus:**

- Incidents + Investigations
- Data + Privacy
- Insurance + Reinsurance

Karla is an associate in the firm's Privacy + Cyber practice. Her daily work includes counseling insureds on the initial incident response, potential ransom payment, restoration, data mining, and notification segments of the incident response practice. She also leads efforts to identifying and remediating shortcomings in cybersecurity and privacy practices of firm clients.

Prior to joining the firm, Karla was a cyber services manager for the Beazley Group, offering proactive risk management guidance to clients seeking to improve their controls and mitigate risks before an incident occurs. Additionally, she has handled more than 500 active cybersecurity incidents.

Karla received her J.D. from LMU Loyola Law School with a concentration in cybersecurity and data privacy and her bachelor's degree in political science from Mount Saint Mary's University, where she graduated *cum laude*.

## Related Practices and Industries

- Privacy + Cyber

## Speaking Engagements

- Panelist, CISO/CSO/General Counsel Summit, Converge Security, Anaheim, CA, September 15, 2023.

## Publications

- Co-author, "California Delete Act: An Aggressive New Approach to Regulating Data Brokers," *Troutman Pepper*, October 19, 2023.
- Co-author, "SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on their Security and Disclosure Plans," *Troutman Pepper*, July 31, 2023.

- Co-author, "A Checklist for Cyber Incident Response Communications," *Law360*, July 14, 2023.

## Professional Experience

- Cyber services manager, Beazley Group, (2021-2023)
- Law clerk, Consumer Protection Unit, (2020)

## Bar Admissions

- California

## Education

- Loyola Law School, Los Angeles, J.D., 2020, LMU Loyola Law School Dean's Service Award
- Mount St. Mary's University, B.A., *cum laude*, 2016, Gibson, Dunn & Crutcher Pre-law Scholarship

## Certifications and Memberships

- Certified Information Privacy Professional/United States (CIPP/US)

## Robyn W. Lin

Associate
Orange County

robyn.lin@troutman.com
D 949.622.2447


Robyn is a privacy and data security attorney who focuses on helping clients understand and maintain data compliance.

**Areas of Focus:**

- Privacy + Cyber
- Consumer Financial Services

Robyn is an associate in the firm's Privacy + Cyber Practice Group. She assists clients with all aspects of their privacy programs, including an initial assessment of applicable law, policy drafting, and implementation. Clients have turned to her for assistance with privacy and security assessments addressing privacy compliance and risk management, including assessments under FTC consent orders. She also serves as a subject matter expert and provides due diligence support for mergers and acquisitions. Robyn focuses her practice on federal and state privacy and security laws, including the California Consumer Privacy Act, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, along with sectoral laws such as Gramm-Leach-Bliley and the Children's Online Privacy Protection Act.

Robyn regularly writes and speaks about privacy and data security issues, and serves as the assistant editor of Troutman Pepper's *More Privacy, Please*, a monthly newsletter recapping industry and legal developments in the areas of cybersecurity, information governance, and privacy.

Robyn earned her J.D. from the University of California, Irvine School of Law where she received the Pro Bono Achievement Award for three consecutive years and was also awarded the Dean's Award in her education law class.

While in law school, Robyn served as a judicial extern for the Hon. Judge Salter of the Orange County Superior Court. Robyn earned her bachelor's degree from Vassar College.

## Related Practices and Industries

- Financial Services

## Speaking Engagements

- Presenter, "Navigating the Complex Landscape of Privacy and Cybersecurity: Emerging Trends, Regulatory Complexities, and Compliance Strategies," myLawCLE and the Federal Bar Association, January 9, 2024.

## Publications

- Co-author, "California Delete Act: An Aggressive New Approach to Regulating Data Brokers," *Troutman Pepper*, October 19, 2023.
- Co-author, "CPRA Shuffle: Two Steps Forward, One Step Back: Court Temporarily Halts CPRA Regulation Enforcement as CPRA Enforcements Begins," *Troutman Pepper*, July 21, 2023.
- Co-author, "Cookies and Online Tracking of Health Signals: An OCR Prescription for Potential Peril," *Troutman Pepper*, May 4, 2023.
- Co-author, "Washington Legislature Goes Big With "My Health My Data Act"," *Troutman Pepper*, May 2, 2023.
- Co-author, "Iowa on Cusp of Enacting Privacy Legislation," *Troutman Pepper*, March 22, 2023.
- Co-author, "BIPA Claims Receive Five-Year Limitations Period," *Troutman Pepper*, February 7, 2023.
- Co-author, "California Age-Appropriate Design Code Is Not Child's Play - Five Practical Tips to Comply and Protect Kids' Privacy," *Pratt's Privacy & Cybersecurity Law Report*, January 2023.
- Co-author, "A Little Breathing Room — California Privacy Agency Modifies Proposed Regulations," *Reuters*, December 8, 2022.
- Co-author, "Silver Lining for Cos. in Proposed Calif. Privacy Law Changes," *Law360*, November 23, 2022.
- Co-author, "California Age-Appropriate Design Code Is Not Child's Play - Five Practical Tips to Comply and Protect Kids' Privacy," *Troutman Pepper*, October 4, 2022.
- Co-author, "Deadline for New UK Contract Requirements for Personal Data Transfers Is Here (EU and California Deadlines Looming)!," *Troutman Pepper*, September 27, 2022.
- Co-author, "Compliance Lessons From Sephora CCPA Settlement," *Law360*, September 13, 2022.
- Co-author, "Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements," *Troutman Pepper*, August 30, 2022.
- Co-author, "CPRA Draft Regulations: Essential Takeaways and Ten Actions to Take Now," *Hedge Fund Law Report*, August 25, 2022.
- Co-author, "California ADCA Bill Aims to Increase Children's Data Privacy," *Security Magazine*, August 24, 2022.
- Co-author, "Simplifying a Complicated Process — Four Steps to Comply with China's PIPL New Security Assessment Requirements for Cross-Border Data Transfers September 1, 2022," *Troutman Pepper*, August 9, 2022.
- Co-author, "CPRA Draft Regulations: Essential Takeaways and 10 Actions to Take Now," *Cybersecurity Law Report*, July 13, 2022.

- Co-author, "California Privacy Protection Agency Publishes Draft Rules," *Troutman Pepper*, June 6, 2022.
- Co-author, "Clearview and ACLU Reach Settlement to Limit Access to Photo Database," *Troutman Pepper*, May 24, 2022.
- Co-author, "Ninth Circuit Provides Guidance on Web Scraping," *Troutman Pepper*, May 5, 2022.
- Co-author, "Connecticut Legislature Passes Comprehensive Privacy Legislation, Awaiting Governor's Signature," *Troutman Pepper*, May 4, 2022.
- Co-author, "Kentucky's Genetic Information Privacy Act Passes," *Troutman Pepper*, April 29, 2022.
- Co-author, "CPRA Series: Part One – Introduction and Overview," *Daily Journal*, April 11, 2022.
- Co-author, "A Fresh "Face" of Privacy: 2022 Biometric Laws," *Troutman Pepper*, April 5, 2022.
- Co-author, "Utah Becomes Fourth State to Adopt Privacy Legislation," *Troutman Pepper*, March 24, 2022.
- Co-author, "2021 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Pepper*, January 28, 2022.

## Professional and Community Involvement

- Board member, Asian Pacific American Women Lawyers Alliance
- Mentor, Sophomore Career Connections, Vassar College (2023)
- Member, Governing Council, UCI Law Alumni Association

## Professional Experience

- Judicial extern, Hon. Judge Salter, Orange County Superior Court, Summer 2019

## Bar Admissions

- California

## Education

- University of California, Irvine School of Law, J.D., 2021
- Vassar College, B.A., 2018

## Whitney L. Shephard

Associate
Boston

whitney.shephard@troutman.com
D 617.443.3709


**Areas of Focus:**

- Regulatory Investigations, Strategy + Enforcement
- White Collar + Government Investigations

Whitney is an associate in the firm's Regulatory Investigations, Strategy + Enforcement (RISE) Practice Group. She represents clients facing state and federal regulatory investigations and enforcement actions, as well as related civil litigation. Whitney regularly provides ongoing commentary and analysis on developments in the state and federal regulatory landscape through the firm's Regulatory blog, Regulatory Oversight.

Prior to joining the firm, Whitney served as compliance program manager for ADP, where she provided support related to complex regulatory and compliance issues presented by the Patient Protection and Affordable Care Act (ACA), in addition to FMLA, FLSA, COBRA, and other laws impacting employers.

*Representative matters may include engagements before joining Troutman Pepper.*

### Related Practices and Industries

- Government + Regulatory
- Health Care Litigation
- Incidents + Investigations
- Public Records/FOIA

### Publications

- Co-author, "A Closer Look at Another HBCU Race Bias Suit Against NCAA," *Law360*, September 7, 2023.
- Co-author, "Making an Impact: State Attorneys General Races in 2023 and Beyond," *Reuters*, September 7, 2023.
- Co-author, "A Checklist for Cyber Incident Response Communications," *Law360*, July 14, 2023.

- Co-author, "Regulating AI: AGs Balance Consumer Protection With Innovation," *The Legal Industry Reviews*, March 30, 2023.
- Co-author, "2022 Regulatory Privacy Year in Review," *Troutman Pepper*, February 2, 2023.
- Co-author, "CPRA Series: Part Two – Consumer Rights," *Daily Journal*, April 20, 2022.

## Professional and Community Involvement

- Victim Assistance Volunteer Court Advocate

## Bar Admissions

- New Hampshire
- Massachusetts

## Court Admissions

- U.S. District Court, District of New Hampshire

## Education

- Charlotte School of Law, J.D., 2014
- James Madison University, B.A., 2010

## Edgar Vargas

Associate
Orange County

edgar.vargas@troutman.com
D 949.622.2473


Edgar is a Certified Information Privacy Professional (CIPP/US). He assists clients on compliance and litigation issues, including issues regarding privacy and cybersecurity laws. He is fluent in Spanish, allowing him to effectively communicate with and serve Spanish speaking clients.

**Areas of Focus:**

- Privacy + Cyber
- Incidents + Investigations

Edgar is an associate in the firm's Consumer Financial Services section, and part of the firm's Privacy + Cyber Practice Group. He develops strategies for clients around issues related to new-to-market and emerging technologies. He also advises on the effective use of data and helps clients mitigate the potential risks associated with the commercialization of data assets. Edgar regularly assists clients with their assessment of, and compliance with, federal and state privacy and security laws, including CAN-SPAM, COPPA, HIPAA, and CCPA; privacy policies, terms of use, information security policies, and data governance agreements, as well as data privacy and security due diligence, and M&A support.

Edgar graduated with his J.D. from University of California, Hastings College of the Law, where he served as the co-editor-in-chief of the *Hastings Science and Technology Law Journal*. During law school, Edgar worked as a law clerk for the U.S. Attorney's Office and served as a judicial extern for the Honorable Daniel A. Flores in the San Francisco Superior Court.

*Representative matters may include engagements before joining Troutman Pepper.*

## Speaking Engagements

- Panelist, CISO/CSO/General Counsel Summit, Converge Security, Anaheim, CA, September 15, 2023.
- Speaker, "Concerns for the Digital Age," Troutman Pepper CLE Webinar, April 19, 2023.
- Speaker, "Beyond a Culture of Fear: The Benefits of Legal and CISOs Uniting in a Post-Uber and Twitter World," MCLE Day, San Francisco, Troutman Pepper, January 24, 2023.
- Panelist, "When the CEO Calls – Part II," Troutman Pepper CLE Webinar, September 29, 2022.

- Speaker, "GDPR – Three Years Later, The Lessons Learned and What's to Come," Troutman Pepper, June 24, 2021.
- Speaker, "Operationalizing the Virginia Consumer Data Protection Act: Leveraging Lessons From the CCPA," 16th Annual Credit and Collection News Conference, April 28, 2021.
- Speaker, "Three Reasons Why 2021 Is a Good Year to Review Your Privacy Compliance Program," Troutman Pepper, March 31, 2021.
- Panelist, "Diverse Perspectives on Careers in Privacy and Cybersecurity," Los Angeles County Bar Association Webinar, February 16, 2021.

## Publications

- Co-author, "Iowa on Cusp of Enacting Privacy Legislation," *Troutman Pepper*, March 22, 2023.
- Co-author, "Did You Suffer a Data Breach and What Are Your Notice Obligations?," *Daily Journal*, March 10, 2023.
- Co-author, "The Safeguards Rule: Protecting Information at Financial Institutions," *Thomson Reuters Westlaw*, January 25, 2023.
- Co-author, "Piecing It All Together: OFAC Combines Seven Years of Regulations, Amendments, and Interpretations All in One," *Troutman Pepper*, September 14, 2022.
- Co-author, "Compliance Lessons From Sephora CCPA Settlement," *Law360*, September 13, 2022.
- Co-author, "Not So Pretty: Five Takeaways from New CCPA Settlement with Sephora and Other Enforcements," *Troutman Pepper*, August 30, 2022.
- Co-author, "California Privacy Protection Agency Publishes Draft Rules," *Troutman Pepper*, June 6, 2022.
- Co-author, "CPRA Series: Part Four – Data Processing Obligation," *Daily Journal*, May 23, 2022.
- Co-author, "Ninth Circuit Provides Guidance on Web Scraping," *Troutman Pepper*, May 5, 2022.
- Co-author, "Connecticut Legislature Passes Comprehensive Privacy Legislation, Awaiting Governor's Signature," *Troutman Pepper*, May 4, 2022.
- Co-author, "Utah Becomes Fourth State to Adopt Privacy Legislation," *Troutman Pepper*, March 24, 2022.
- Co-author, "2021 Consumer Financial Services Year in Review & A Look Ahead," *Troutman Pepper*, January 28, 2022.
- Co-author, "New Standard Contractual Clauses Supply Opportunities and Obligations for Organizations Transferring Personal Data Out of the EU," *Troutman Pepper*, July 22, 2021.
- Co-author, "Introduction and Overview: Virginia Consumer Data Protection Act Series (Part One)," *Troutman Pepper*, March 4, 2021.
- Co-author, "DFS Releases its Cyber Insurance Risk Framework," Troutman Pepper Consumer Financial Services Law Monitor, February 16, 2021.
- Co-author, "Data Compliance Issues for Cos. Making, Using Vaccine App," *Law360*, February 10, 2021.
- Co-author, "The FTC Hosted its Workshop on the Proposed Changes to the Safeguards Rule," Troutman Pepper Consumer Financial Services Law Monitor, July 20, 2020.

- Co-author, "CISA Shares 5 Ways a Business's Staff Could Reduce Their Cyber Risks," Troutman Pepper Consumer Financial Services Law Monitor, July 7, 2020.
- Co-author, "FTC Settles With App Developer Over Allegations of Unlawfully Processing Children's Information," Troutman Pepper Consumer Financial Services Law Monitor, June 9, 2020.
- Co-author, "CISA Shares 5 Ways Business Leaders Could Reduce Their Organizations' Cyber Risks," Troutman Pepper Consumer Financial Services Law Monitor, June 8, 2020.
- Co-author, "FTC Settles With Online Game Developer Regarding Allegations Concerning Children's Privacy," Troutman Pepper Consumer Financial Services Law Monitor, May 21, 2020.
- Co-author, "Calif. Privacy Law Takeaways From 9th Circ. Facebook Case," *Law360*, April 27, 2020.
- Co-author, "Calif. AG's Latest Privacy Law Revisions Miss Some Spots," *Law360*, March 19, 2020.
- Co-author, "FTC Will Accept Additional Comments on Proposed Amendments to the Safeguards Rule," Troutman Pepper Consumer Financial Services Law Monitor, March 16, 2020.

## Professional and Community Involvement

- Orange County Bar Association
- Los Angeles County Bar Association
- International Association of Privacy Professionals

## Professional Experience

- United States Attorney's Office, 2018
- Judicial extern, Honorable Daniel A. Flores, San Francisco Superior Court, 2017

## Bar Admissions

- California

## Education

- University of California College of the Law, San Francisco, J.D., 2019, co-editor-in-chief, *Hastings Science and Technology Law Journal*
- California State University, Long Beach, B.A., 2015

## Languages

- Spanish