




BakerHostetler

2025 DATA SECURITY INCIDENT RESPONSE REPORT

Ready and Resilient in the Data-Driven Age

Featuring Insights from the
Digital Assets and Data Management Group



Key Findings



Ransomware Decline.

We see fewer attacks and lower payments. After several chaotic years, ransomware is settling into the category of risk that still exists but for which there are known measures that should make an impactful attack less likely.



More Revenue, More Ransom? Nope.

Entity revenue does not correlate to ransom payment amount. The impact of a ransomware event is the bigger driver of payment amount.



Healthcare Under Siege.

Year in and year out we see the most incidents involving our healthcare clients. Once again, we observed disruptions to patient care and losses in revenue.



Up Your Crime-Fraud Limits (Or Use Good Authorization Measures).

It wasn't \$5 here and \$10 there. Wires in the millions fueled a three-fold increase in the total amount of fraudulent fund transfers (the average wire was over \$1M).



And It's Not Just Gift Cards for the CEO.

Threat actors use a slew of social engineering techniques, including spear phishing, vishing, social engineering of help-desk employees, MFA bombing, and more. User training must adapt.



Human Error and Poor Cyber Hygiene Still Drive Incidents.

Despite the availability of strong security controls, attackers are still getting in through the same old methods (phishing, social engineering, unpatched devices, assets without access restrictions) due to ineffective implementation or human error.



Who Needs Malware?

With admin credentials, threat actors don't need malware after gaining entry to an environment — they're quite content (and undetected) living off the land (using techniques like LOLBins).



Half Measures ≠ Effective Prep.

Your organization finally prepared an IRP and a BCP. That's great! But have you actually implemented and then tested these plans?



Forensic Costs Are Down (Again).

EDR deployment prior to an incident and decreased malware use during an incident led to faster containment and investigations, bringing costs down for the third year in a row.



Hate to Say We Told You So.

Last year's DSIR Report noted the "Rise of the Risk Assessment." This came to fruition for HIPAA-covered entities in late 2024, when the OCR formally announced its Risk Analysis Initiative and the first set of associated penalties.



Where Is the AI?

Artificial intelligence — it shows up in technology but has not shown up prominently in attacks...yet.



Tip of the Cap.

Law enforcement agencies around the world continue to work together to score meaningful wins against threat actors (like Scattered Spider).



Materiality Is Rare.

For public companies, most security incidents are not "material." Fewer than 1% of our public company matters resulted in an 8-K filing.



U.S. as Crypto Capital of the Planet!

Expect to see pro-digital asset policies in 2025.



No Magic Bullet for Vendor Incidents.

However, vendor management programs are still critical in mitigating risk.



Payment Card Incident? What's That?

Payment card incidents, which used to have significant impact, have all but disappeared due to P2PE and EMV.



We Know It's the VPN; We Just Don't Know How.

Insufficient logging makes it hard to determine whether initial access through the VPN occurred by exploiting a vulnerability, using compromised credentials, or executing a brute force attack.

Table of Contents

- 01.** Letter to Clients & Friends of the Firm
- 02.** Incident Response Trends — At a Glance
- 03.** Industries Affected
- 04.** Incident Response Life Cycle
- 05.** Deeper Dive into the Data
- 06.** Data Privacy Litigation Trends
- 07.** Web Tracking/Pixel Litigation & Regulatory Landscape
- 08.** OCR/Healthcare
- 09.** Securities & Exchange Commission
- 10.** Global Privacy
- 11.** State Comprehensive Privacy Laws
- 12.** Information Governance
- 13.** Federal Trade Commission
- 14.** Digital Assets
- 15.** Artificial Intelligence

CHAPTER 01

Clients & Friends of the Firm

Welcome to our 11th annual Data Security Incident Response Report!

The idea for this report came from spending time on-site with clients and watching them leverage not only their data but also our data — to predict outcomes and make decisions during a cybersecurity crisis response. It's rewarding to see clients and third-party partners refer to the report during the year. A chief legal officer reassuring a board that the right vendors have been retained can go a long way, and when that executive can provide actual industry-specific averages for time to restore, ransom payment amounts, and number of individuals notified, the board gets even greater comfort and likely is better prepared to ask the questions necessary as part of its oversight responsibility.

It is hard to believe that it has been six years since we became (and remain) the only law firm to create a practice group — our Digital Assets and Data Management (DADM) Practice Group — dedicated to lifting data, technology, and innovation to the same level as traditional law firm practice groups to advise clients across the life cycle of data and technology. Building a convergence practice enabled us to more effectively help clients address enterprise risks and opportunities involving data, brand strategies, and innovation. Seeing how threat actors attack assets, regulators build enforcement priorities, private litigants choose whom to pursue and how to resolve claims, and entities build and market products and services allows our team to provide practical and actionable advice tailored to risk appetite and goals.

We are now building our group's second five-year strategic plan, and our planning highlights the underlying challenge in this area: The more things change, the more they stay the same. Yes, there are definitely areas of rapid change. We see AI creating disruption, yet it has not shown up in a meaningful way in security incidents. Phishing was the leading underlying cause of incidents in our first report, 11 years ago (at 31%), and it is still near the top of the list this year (24%) (however, it has evolved — our report covers four different tactics). Phishing awareness training has not eradicated phishing as an effective attack vector, though there are definitely areas where the security industry has made progress. The industry supporting compromised entities has matured — as a result, we see shorter dwell time, shorter time to containment, faster completion of forensic investigations, lower cost for forensic investigations, shorter time to restoration after ransomware deployment, and declining ransom payment amounts. The combined efforts of carriers, brokers, law firms, forensic firms, restoration firms, ransom negotiation and payment facilitation firms, and law enforcement have yielded positive results.

An area where more help is warranted is post-data breach lawsuits and privacy lawsuits (especially ones exploiting old laws because those laws have minimum statutory damage components). After 15+ years of sensitive data being compromised, the records of most individuals have been involved 5, 10, or 50 times. Consequently, it is extremely rare to see actual fraud or loss connected to an incident. In the absence of harm, it is disappointing to see litigants capitalize on the uncertainty caused by old laws and inconsistent rulings for financial gain. The value of both precedent and the rule of law is immeasurable.

We hope you enjoy the report, and we invite you to reach out to any one of the DADM Practice Group's members with questions or suggestions.

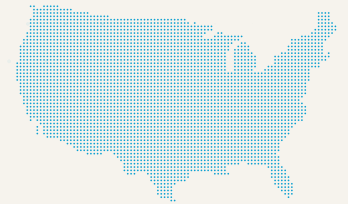
Sincerely,



Ted Kobus

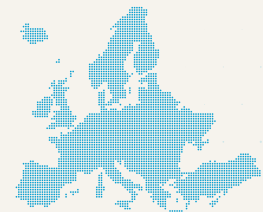
1,250+

INCIDENTS IN 2024



U.S. Data Breach Notification Law Interactive Map

bakerdatacounsel.com



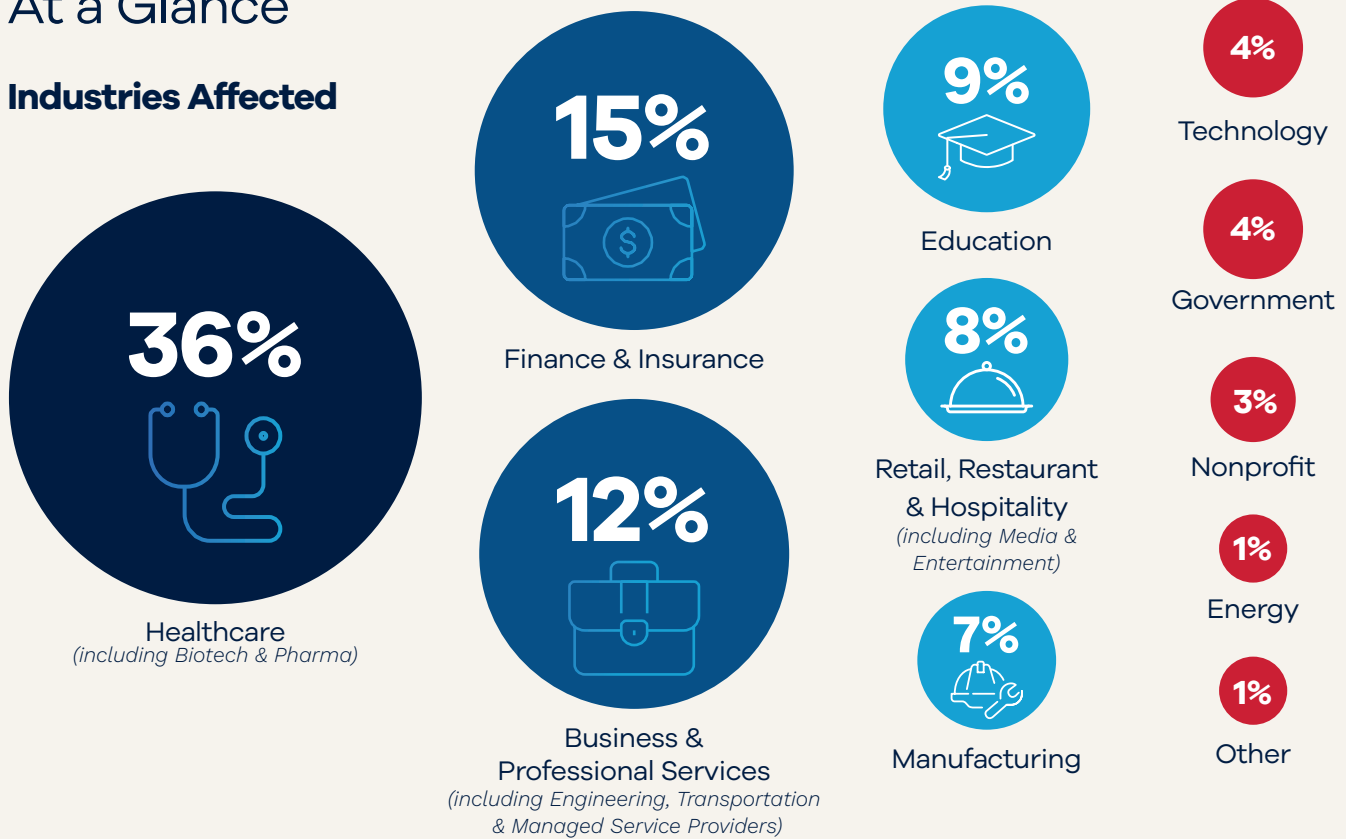
EU GDPR Data Breach Notification Resource Map

bakerdatacounsel.com

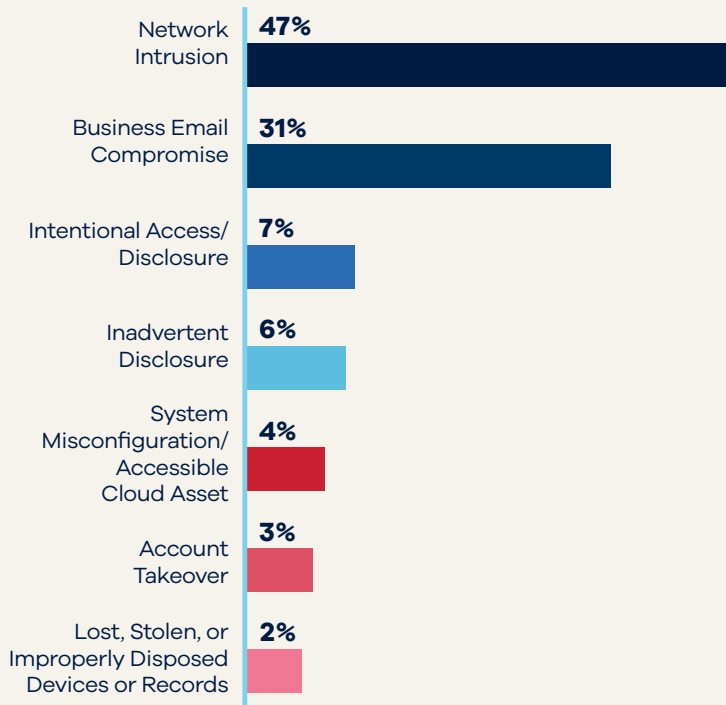
Incident Response Trends

At a Glance

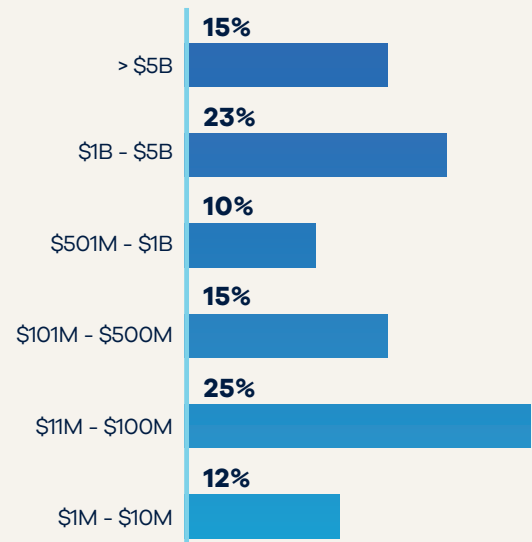
Industries Affected



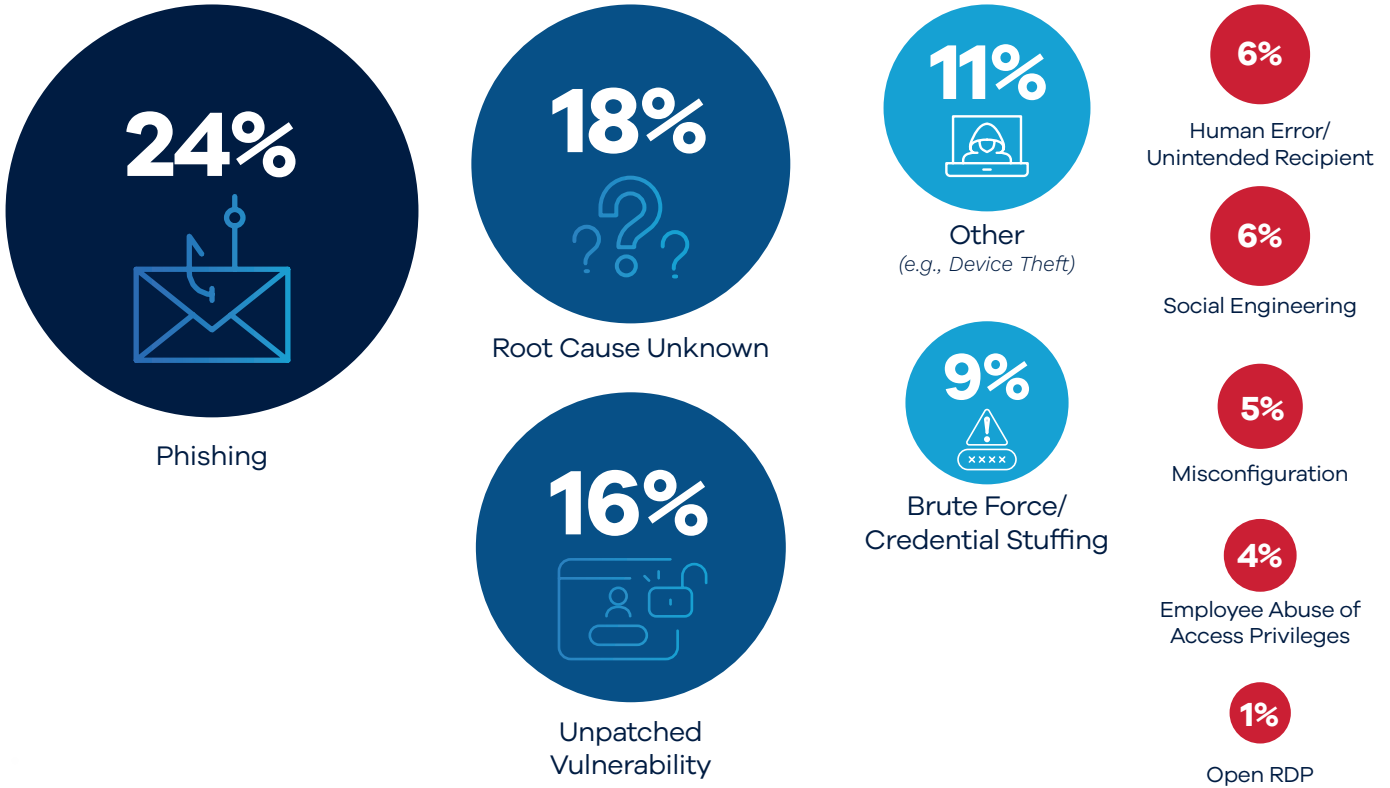
Incident Type



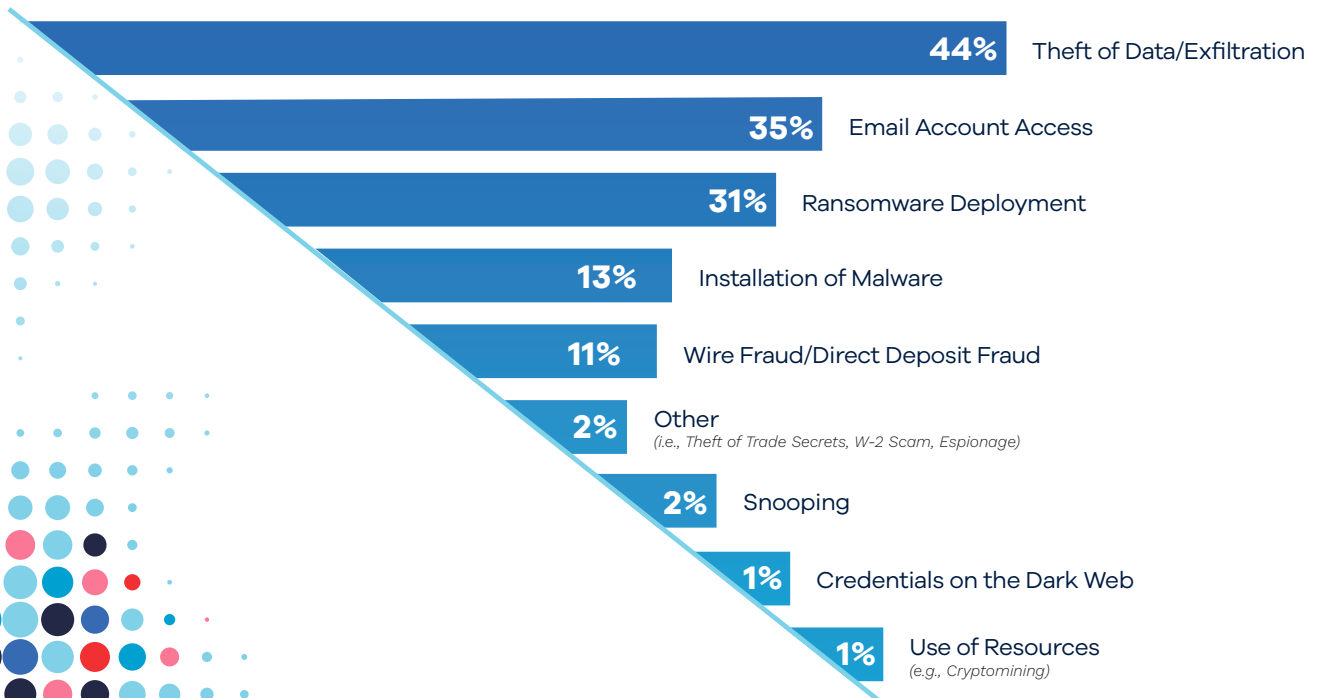
Entity Size by Annual Revenue



Root Cause
All Incidents



What Happens Next
All Incidents



Incident Response Timeline (Median)



Occurrence to Discovery



Discovery to Containment



Time to Complete Forensic Investigation



Discovery to Notification

Forensic Investigation Costs (Average)

\$41,145

All Incidents

\$70,367

Network Intrusion Incidents

\$273,260

20 Largest Network Intrusion Incidents

Ransom Demand & Payment (Average)

\$2,502,565

Ransom Demand (all Industries)

\$916,203

Ransom Payment (all Industries)

\$501,338

Ransom Payment (excluding largest payment [\$20M] from average)

The average ransom paid dropped by **33%** to **\$501,338.**

Wire Fraud

\$109,341,352

Total Amount of Fraudulent Wire Transfers

32%

Matters that Recovered Funds (totaling over \$49.5 million)

\$1,256,797

Average Wire Transfer

\$130,000

Median Wire Transfer

\$20.6M

Largest Wire Transfer

\$1,707,837

Average Recovery

\$112,448

Median Recovery

The total value of fraudulent fund transfers increased by **211%**

Notifications Leading to Lawsuits & Regulatory Inquiries

518

Notifications
(42% of matters)

33,286

Average Number of
Individuals Notified

112

Regulatory
Inquiries

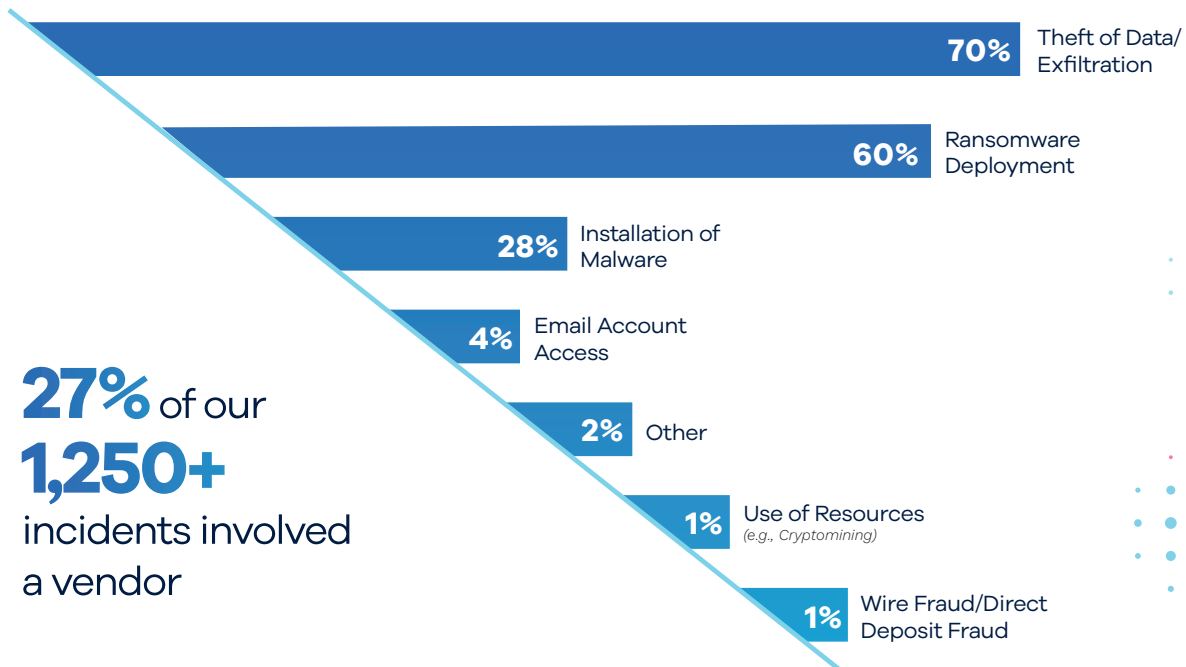
51

Incidents
with Lawsuits

Root Cause Network Intrusions



What Happens Next Network Intrusions



Industries Affected

● Average ● Median ● Largest

Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
BUSINESS & PROFESSIONAL SERVICES				
\$2,184,074 \$775K \$15M	\$352,811 \$250K \$1M	9.1 9	\$35,165 \$14.5K \$330K	1,252 104 19K
EDUCATION				
\$996,543 \$725K \$1M	\$98,948 \$98,948 \$100K	13.4 10	\$53,878 \$35,488 \$318K	2,088 249 18.7K
ENERGY & TECHNOLOGY				
\$1,852,856 \$303K \$10M	\$235,139 \$111K \$750K	10.1 7	\$60,981 \$33.6K \$241K	16,653 1,300 96K
FINANCE & INSURANCE				
\$6,997,473 \$285K \$40M	\$6,750,749 \$150K \$20M	8.4 7	\$29,895 \$10.5K \$590K	33,236 409 2.158M
GOVERNMENT				
\$544,906 \$650K \$1M	\$600,000 \$600K \$600K	13 12	\$48,775 \$34,275 \$148K	1,007 513 4K
HEALTHCARE				
\$1,889,573 \$1.4M \$7M	\$847,875 \$375K \$2.5M	27.2 24	\$36,314 \$14,750 \$226K	58,520 876 2.151M
MANUFACTURING				
\$4,951,440 \$1.75M \$28.7M	\$562,857 \$180K \$3M	10.3 10	\$49,784 \$21,575 \$439K	1,379 263 23K
NONPROFIT				
\$187,500 \$187.5K \$350K	\$150,000 \$150K \$150K	7 7	\$19,767 \$10.5K \$114K	2,585 47 16K
RETAIL, RESTAURANT & HOSPITALITY				
\$2,360,071 \$1.95M \$8.2M	\$840,286 \$743.5K \$1.8M	9.3 9	\$50,482 \$34,133 \$240K	81,384 400 1.96M

Incident Response Life Cycle

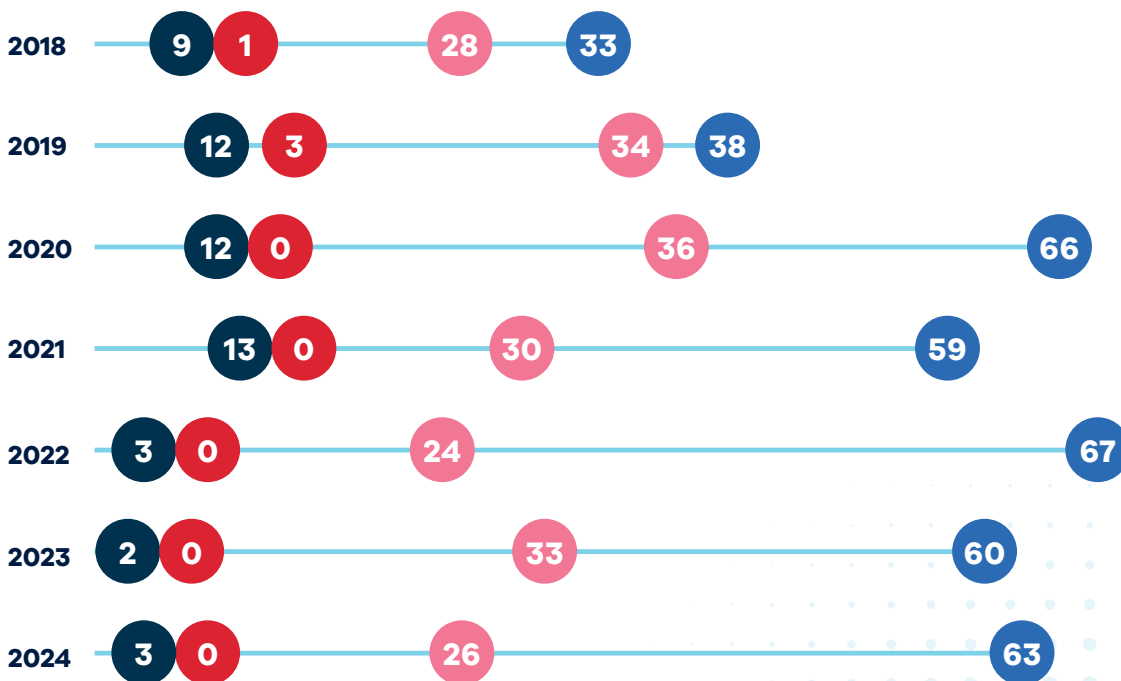
Incident Response Timeline *(in Days)*

	Detection Occurrence to Discovery	Containment Discovery to Containment	Analysis Time to Complete Forensic Investigation	Notification Discovery to Notification
Median All Incidents	3	0	26	63
Average All Incidents	31	4	34	77
Average Network Intrusions	26	5	33	74

Incident Response Timeline

Look Back *(Median in Days)*

● Detection ● Containment ● Analysis ● Notification



Deeper Dive into the Data

Largest Ransom Demand in 2024:

\$40+ Million

(\$30+ Million in 2023)

Largest Ransom Paid in 2024:

\$20+ Million

(\$10+ Million in 2023)

Average Ransom Paid in 2024:

\$916,203

Ransom Payment (all Industries)

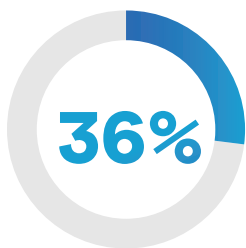
\$501,338

(\$747,651 in 2023)

Ransomware Timeline (in Days)

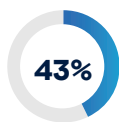
● Average ● Median

	Demand to Payment	Demand to Payment for Payments <\$1M	Demand to Payment for Payments > \$1M	Encryption to Restoration
2020	8	7.4	9.2	13
2021	11.1	13	9.8	12.2
2022	14.2	14	14.9	12.7
2023	16.6	16.3	18.3	11.9
2024	15.4 <small>12</small>	10.2 <small>9</small>	21.9 <small>23</small>	14.2 <small>10</small>

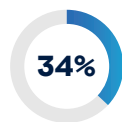


of ransomware/ extortion victims paid a ransom

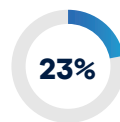
The primary reasons for payment are:



to buy a decryptor



to prevent the publication of the stolen data



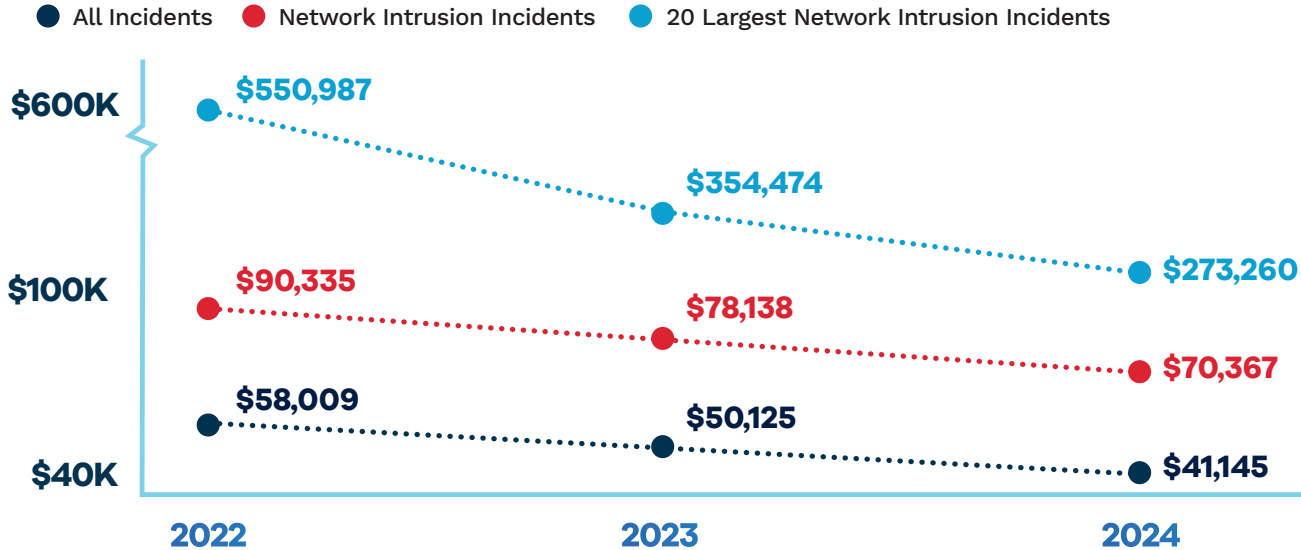
for both a decryptor & to prevent publication of the stolen data

62%

of ransomware/ extortion incidents involved theft of data resulting in notice to individuals

Forensic Trends

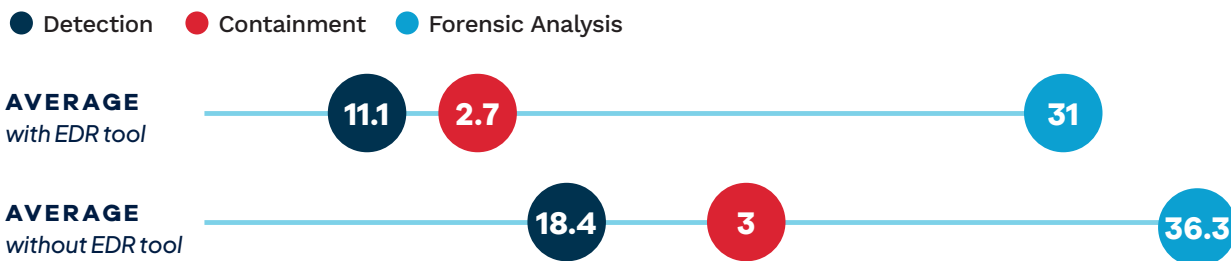
Average Forensic Investigation Costs



Forensic investigation costs continue to drop, marking a three-year low and a 30% reduction in cost. The same factors we identified last year are, in combination, driving forensic costs down:

- 01. EDR & Triage Tools:** The use of EDR tools that were deployed pre-incident and triage collection tools allow for quick and broad assessment of systems to focus on, reducing the need for full disk image review.
- 02. SIEM | Cloud | Virtualization:** It is now easier to access and obtain host and network logs.
- 03. Maturing Industry:** There are more forensic firms, and competition has affected rates and driven innovation.
- 04. Experience-Driven Efficiency for BECs:** The median investigation fee for a BEC incident was \$8,500.

Network Intrusion Timelines With and Without EDR (in Days)



Even better, we observed that having EDR in place prior to an incident led to faster detection (by over seven days on average) and a faster and, therefore, less expensive forensic investigation (almost 15% shorter on average).

Don't Just Contain — Strengthen Overall Security Posture

Common questions during and in the aftermath of a security incident focus on what allowed the incident to occur. Initial containment measures focus on identifying and correcting the root cause (or aggressively locking down the network when the root cause is unknown). A strong incident response approach does not stop there. It is hard to do in the middle of the investigation but building a plan to identify short- and long-term security enhancements is key to preventing similar issues from occurring in the future and meeting customer (both consumer and commercial) and regulatory expectations.

Below are common areas on which to focus when building a post-incident security enhancement plan:

Insufficient Identity and Access Management

Organizations can reduce their risk by narrowing access permissions to the minimum necessary for a user's role. That way, if an account is compromised, the threat actor has access to only the data and applications necessary and accessible to that user.

Stockpiles of Old Data

Clients are often shocked to learn that files from 25+ years ago were stored on the File Share or that Jane in Accounting had been exporting and locally saving a monthly payroll report containing all current employees' and dependents' names and SSNs for the last several years. Putting in place an appropriate data retention policy, identifying and deleting data consistent with that policy, and limiting where sensitive data is stored are big risk reduction measures.

Incomplete Logging

Insufficient logging can make it difficult to identify — and effectively address — the root cause of an incident (forensic firms could not determine the root cause in 18% of our matters). Insufficient logging can also lead to difficulties identifying all the systems and data accessed by the threat actor during an incident. This can result in having a higher notice population (because there's a lack of visibility into the exact files taken), which can, in turn, lead to increased litigation and regulatory risk or difficulties answering auditors' questions (because it's unknown what the threat actor did on financial systems).

Lack of EDR or Flawed EDR Deployment

EDR (and managed and extended detection and response — MDR and XDR) cannot detect what it cannot see. EDR works extremely well but must be deployed throughout an entire network, including to all workstations, with 24/7 monitoring. But deployment isn't enough — EDR must be configured correctly with anti-tampering settings in place.

Too Much Privilege

Companies should audit accounts to remove higher privileges than are necessary for each user's role. If a threat actor accesses a "regular" account, the threat actor shouldn't be able to create new accounts or add or change MFA assets — all methods by which threat actors maintain persistence and expand access.

No MFA

At a minimum, MFA should be enforced for remote access as well as privileged and administrator accounts. Although MFA isn't foolproof, it remains an essential tool in helping to prevent unauthorized access to systems and data.

Ransomware Chaos Persists but Prevalence and Impact Reduced

From law enforcement takedowns to ransomware-as-a-service (RaaS) developers cheating out affiliates, all bets were off in 2024!

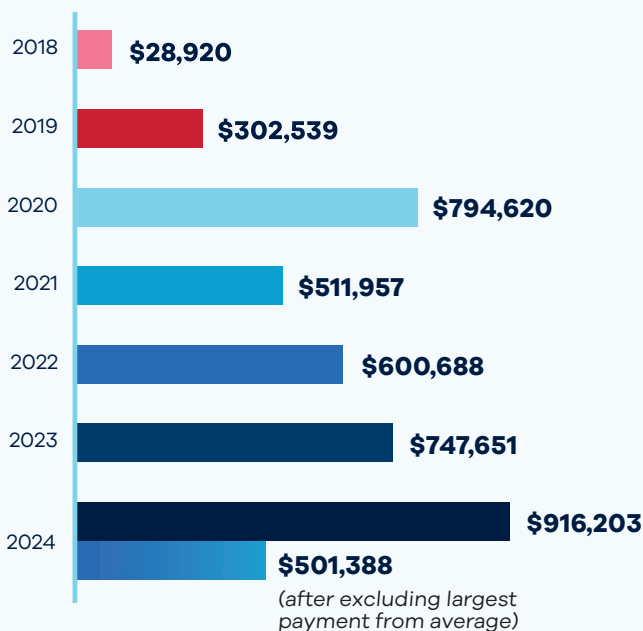
Q1 of 2024 started strong with the February announcement that the FBI, DOJ, and international law enforcement agencies disrupted LockBit's operations by seizing its infrastructure. It was a worthy target — LockBit is the only group that has been in the top five most active groups for the past four years.

Over the next several months, U.S. and international agencies imposed formal sanctions, offered big rewards, and made arrests of individuals associated with LockBit, Scattered Spider, Phobos, the BreachForums hacking website, and more. Notably, law enforcement's actions extended beyond just developers of ransomware (those who design the actual code and maintain the operational infrastructure) but also focused on affiliates (those that carry out the attacks). This pressure led to payment disputes among developers and affiliates, including BlackCat's apparent "exit scam," where it claimed to have been taken down by law enforcement after receiving an infamous \$22M ransom payment and then pocketing the payment without splitting fees with the affiliate that conducted the attack. The affiliate then partnered with another group, RansomHub, to publish data and re-extort the victim.

This disruption created openings for new players willing to accept smaller payment amounts as they built their business. When removing two large outlier demands made before the February 2024 activity discussed above, our clients' average ransom demand in 2024 drops from \$2,502,565 to \$2,004,793, which is a 24% reduction from 2023 (\$2,644,647). The same is true for average payments. When removing a large outlier payment made in connection with a pre-February 2024 incident, the average amount paid drops significantly, from \$916,203 to \$501,388, which is much less than the \$747,651 average we saw in 2023.

LOCKBIT was the only ransomware group to stay in the top five most active threat actor groups for four years — until its takedown in February 2024 followed by a wave of other groups' sanctions, arrests, and cybercriminal infighting.

Average Ransom Payment



Average Payment by Primary Reason

Obtain Decryptor

\$335,428

Data Deletion/Suppression

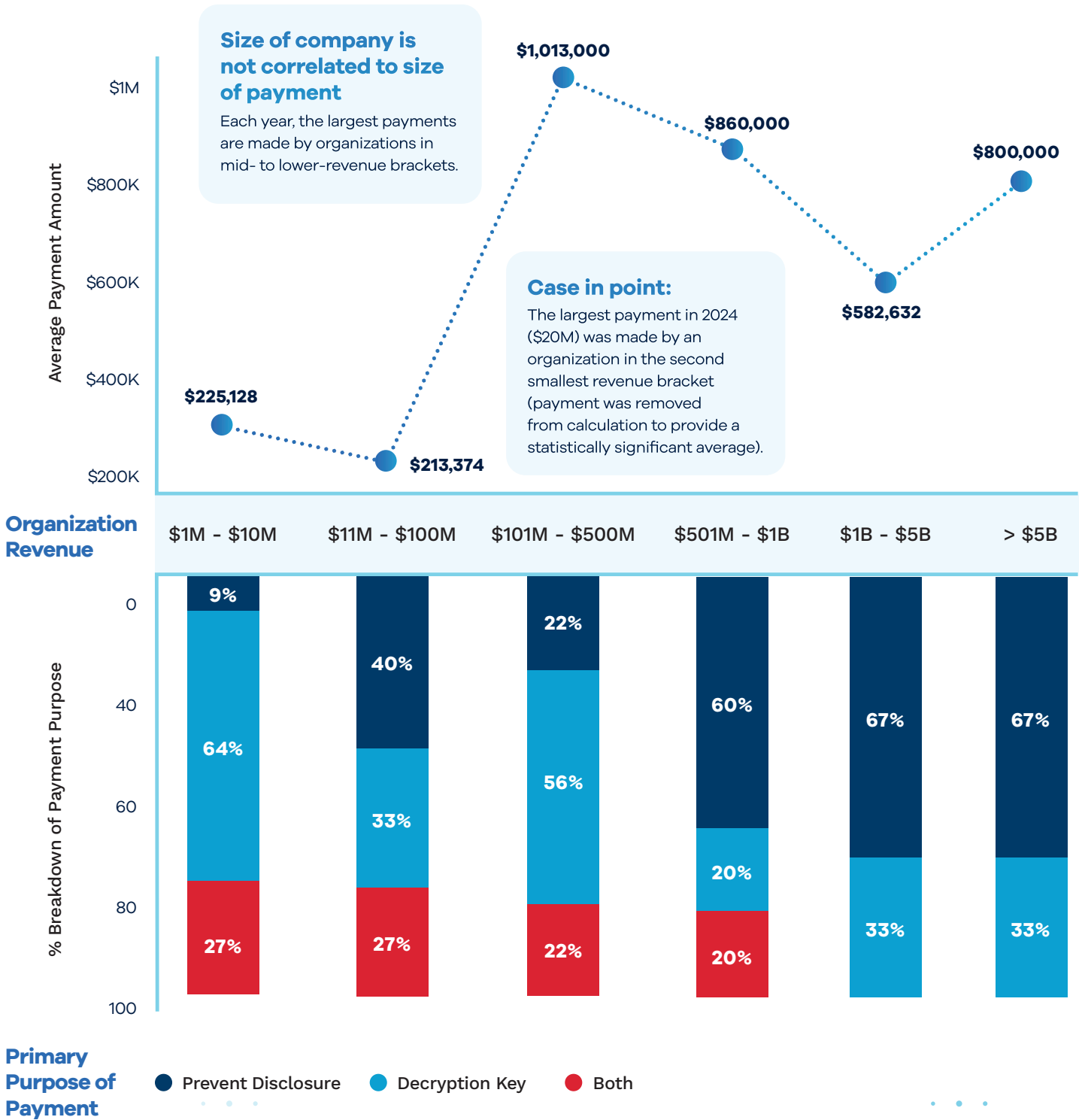
\$626,000

(\$1.8M when including largest payment in average)

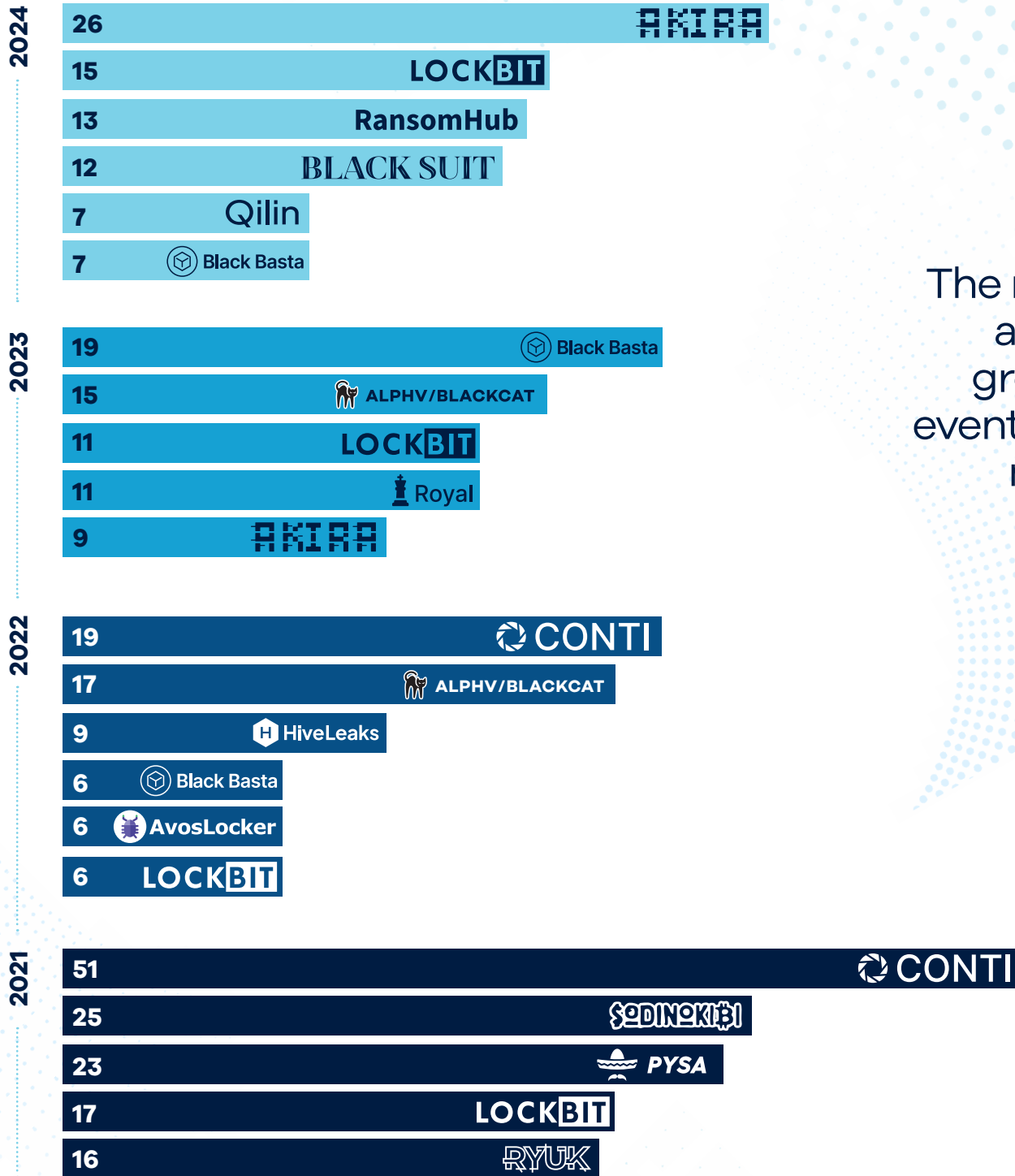
Both

\$633,000

Average Payment and Primary Purpose of Payment by Organizations' Revenue



Most Active Ransomware Groups 2021-2024



The most active groups eventually meet their end.

The number at the left of each bar represents the number of incidents we handled involving the threat actor group.

Social Engineering in Cybersecurity

The most advanced security tools and sophisticated defensive methods cannot completely safeguard against the most insidious vulnerability: human nature. Social engineering — the art of manipulation — exploits trust, urgency, familiarity, and fatigue to bypass security measures. From phishing or spear phishing emails to the social engineering of help-desk employees, attackers continue to refine their techniques, exploiting people as the weakest link in an organization’s cybersecurity defenses.

Social engineering attacks exploit cognitive biases such as authority bias (trusting someone perceived as an authority figure), urgency bias (acting quickly under pressure), and familiarity bias (responding positively to someone recognized as a co-worker). Social engineering attacks often are designed to evoke an emotional reaction — whether it is fear of losing account access or a sense of duty to comply with an urgent request from a “supervisor” or respond to an urgent need for assistance from a co-worker.

The Evolution of Social Engineering Techniques

Modern-day cybercriminals do not rely only on run-of-the-mill phishing emails. Today’s attackers use a vast arsenal of tactics to manipulate individuals and infiltrate organizations:



Spear Phishing

Attackers use targeted attacks crafted using specific and/or personal details related to individuals or organizations to appear legitimate.



Vishing (Voice Phishing)

Attackers use phone calls, sometimes employing AI-generated voices, to impersonate supervisors, colleagues, or IT staff members — commonly seen deployed against help desks to facilitate credential compromises.



Quishing (QR Code Phishing)

Attackers embed malicious QR codes in invoices, emails, or other digital documents.



Pretexting

Attackers create fabricated scenarios often sourced from publicly available information to obtain sensitive information that can be used to induce a fraudulent payment — such as posing as a new or existing vendor needing immediate payment.

These tactics work because they exploit trust, urgency, familiarity, and fatigue. Employees, customers, and vendors can fall victim to attackers masquerading as legitimate contacts.

Mitigation

Technology in isolation cannot stop social engineering attacks. In addition to technology, organizations should employ a multi-layered defense strategy that includes human-centric measures:



MFA

MFA is a critical barrier against unauthorized access even when credentials are compromised. Organizations should require MFA and educate and evaluate employees regarding MFA fatigue — not approving MFA prompts without verifying their legitimacy, especially when faced with a barrage that may be from a threat actor.



Phishing-Resistant MFA

Phishing-resistant MFA is a security method where a physical device, like a USB key or a smart card, is used to generate a unique code or perform a cryptographic operation, providing an extra layer of security beyond traditional MFA (e.g., app or SMS). One of the three primary types of authentication, the key or card functions as something-you-have authentication, whereas passwords are something-you-know authentication, and biometrics, like fingerprints, are something-you-are authentication.



Security Awareness Training

Organizations should require MFA and educate employees regarding MFA fatigue — not approving MFA prompts just because they receive multiple requests.



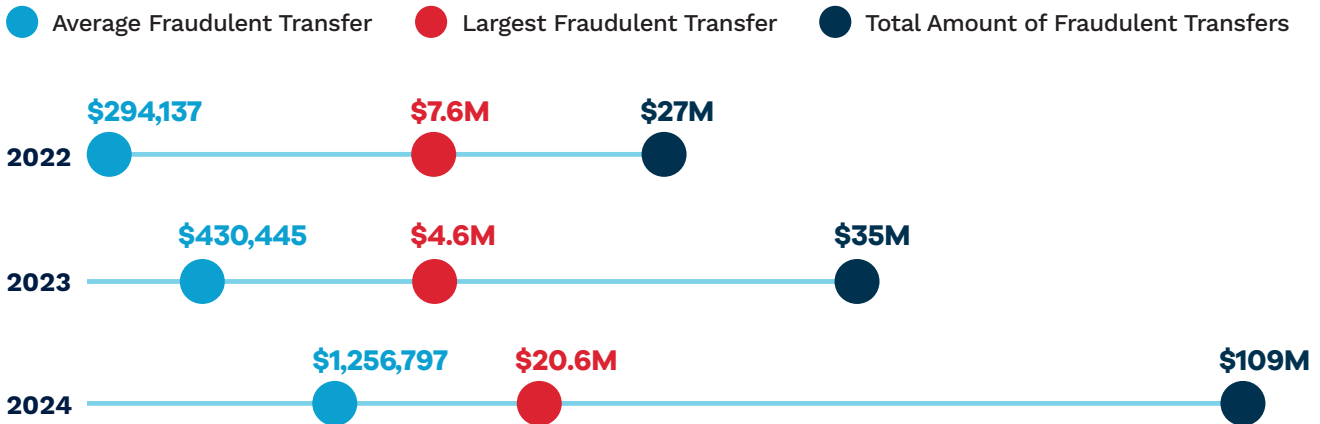
Strong Verification Policies

Organizations should implement strict verification procedures for sensitive requests, such as financial transactions or password resets, including requiring video calls to verify the identity of the requesting person.

Attackers will continue to leverage and evolve social engineering attacks as long as humans remain exploitable weaknesses of cybersecurity programs. Awareness, skepticism, training, and testing are critical components of mitigating these risks because the most effective defense against social engineering is an aware, skeptical, well-trained, and battle-tested human working in conjunction with forward-leaning technical safeguards.

Back to the Basics — Fraudulent Funds Edition

The dollars lost through successfully diverted wires, direct deposits, or ACH payments surged exponentially in 2024:



Although we saw fraudulent fund transfers across all industries in the past year, the Business & Professional Services and Finance & Insurance industries (perhaps expectedly) were targeted the most, with just over 50% of our wire fraud matters affecting clients in these two industries. These industries also made a majority of the high-value (> \$1M) transfers, giving threat actors a sizable return on investment.

Additionally, the median time from initial account access to discovery of the fraudulent fund transfer was significantly higher when compared to all incidents generally (18 days compared to 3 days). As the length of time between the fraudulent transfer and its discovery increases, the likelihood of recovering the funds decreases.

Organizations need to employ both manual and automated verification measures at every stage of the payment process. Though still necessary components, training employees and requiring verbal confirmation for any changes in banking information are no longer sufficient. For example, organizations should also test employees' understanding of policies and procedures, including a post-transfer confirmation step in their overall process; ensure all applicable departments bear responsibility for preventing fraudulent fund transfers; and implement enhanced verification processes for any large, unusual, or new transaction.

The Secret Service's Global Investigative Operations Center (GIOC) — which has been a key partner in recovering funds for our clients — recently began prioritizing investigations for larger and more recent fraudulent fund transfers. While all fraudulent fund transfers should still be reported, the GIOC will focus on those that occurred more recently and involved amounts **greater than \$10,000**.

Vendors Are a Hard Problem to Solve

“You are only as secure as your least-secure key vendor.” If that wasn’t part of the lexicon before, it should be now.

Vendors were the source of 27% of the matters we handled. Between Change Healthcare, Snowflake, and cIOP’s latest in a multi-year string of attacks on secure file transfer protocol applications (SFTPs) (such as Accellion, MOVEit, and now Cleo, among others), vendor incidents persist as a significant risk to all organizations. Third-party risk management should be an essential component of any information security program.

You are only as
secure as your
**least-secure
key vendor.**

Take Action: Build a Vendor Management Program

There is no magic bullet. A vendor management program can provide an important governance structure to enable the use of risk assessment/risk ranking criteria and prioritization analysis to address risks from regular and critical vendors. The program can have three basic parts: (A) pre-selection diligence, (B) contractual standards, and (C) performance oversight (and offboarding) along with enhanced components for critical vendors. The program uses a written policy to describe the method for managing vendors along with standards and guidelines for implementing the three phases of the program. The program can define risk tiers (even as simple as regular and high-impact/critical) to manage the level of effort and intensity of the diligence, obligations to impose, and oversight to use.

Pre-Selection Diligence

When assessing vendors to engage, companies should first classify the level of risk of each vendor (regular, critical, etc.) and then use various assessment methods to help paint a picture of the overall risk exposure presented by the vendor:

1. **Self-assessment questionnaires** (to be completed by the vendor), the details of which can be tailored depending on the criticality of the specific vendor;
2. **Onsite reviews**, to assess physical security controls, interview relevant personnel, and collect artifacts supporting security controls;
3. **Review of regulatory and audit artifacts**, such as a SOC2 assessment report and internal audit reports;
4. **Commercially available third-party risk scoring tools**, which provide insight into a vendor’s financial, cybersecurity, and supply chain risks; and
5. **Open-source intelligence (OSINT)**, which is publicly available and accessible information (such as internet searches, dark and deep web searches, media searches, and commercial suppliers of business information).

Contractual Standards

The program can use short- or long-form contract addenda to address privacy and security issues. Tables based on record volume, data elements, and business continuity importance can be developed to guide contract professionals in negotiating key items like limits of liability and service-level agreements.

Performance Oversight (and Offboarding)

During the relationship, oversight of vendors is key. The oversight program can include steps such as audits and surveys, on-site or remote reviews, annual requests for certifications, identification of scope changes (and reassessment of risk if necessary), incident management (such as notification of a security incident), and review of the overall performance of the vendor. Additionally, vendor offboarding is an often-overlooked component of a vendor management program but is equally important to the other stages. Too often, companies are notified by vendors that the companies’ data was taken in a security incident, even though they had ceased all business with the vendor years prior. The program can define how to close out an engagement (e.g., disabling accounts and connections, returning equipment, and deleting data) to mitigate vendor-related risks going forward.

Notable 2024 Resolutions

\$4.5M

penalty in a ransomware settlement across three state attorneys general.

\$52M

settlement following a hospitality company incident.

\$20M

multistate settlement in the mortgage industry.

\$450K

settlement with a state attorney general for a healthcare incident.

Regulatory Fines

Determining whether regulatory investigation outcomes reveal a trend or an outcome driven by the unique circumstances of the incidents is more art than science. We were part of bringing resolutions to multiple matters in 2024 that involved millions of dollars in fines. Part of the challenge in identifying trends is the time to resolution: for our matters that concluded in 2024, the timeline from incident disclosure ranged from one to six years. Looking at the injunctive relief terms in consent orders is a great way to identify the regulatory view of “reasonable security.” But an issue that allowed an incident to occur many years ago that gets highlighted as a key injunctive relief term in a consent order often is no longer a challenge for most companies by the time the order is published.

For the larger multistate attorney general group consent orders over the past decade, the median time to resolution was 3.5 years. Now attorneys general's offices are more experienced and have larger teams. So, we expect to see more inquiries and faster resolutions. Most large incidents have an obvious post-incident lesson learned (e.g., patching). Identifying the common methods used by attackers, the items that lead to consequential impact, and regulatory outcomes is the recipe for prioritizing security and business resiliency enhancement measures.

Data Privacy Litigation Trends



1,250+

Incidents Handled in 2024



518

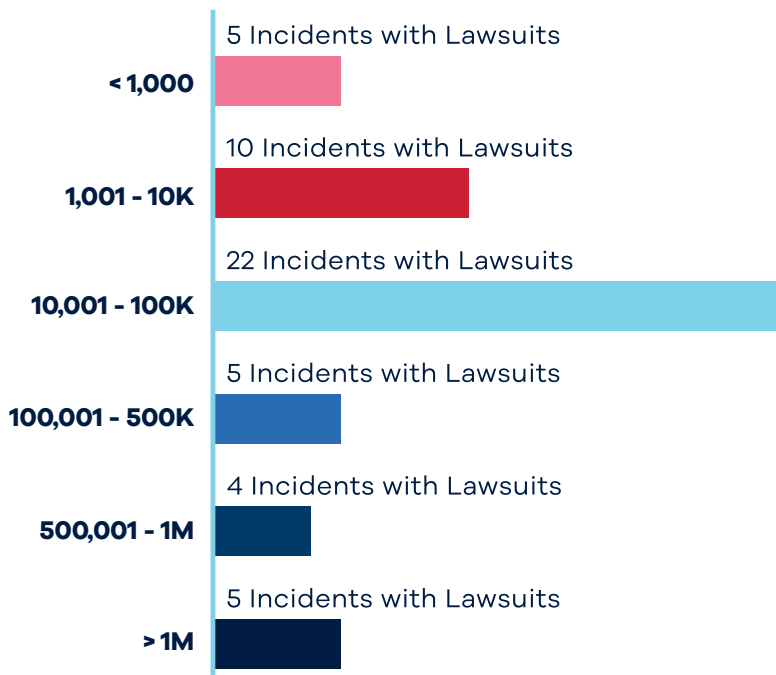
Incidents with Notification



51

Incidents with Lawsuits

Number of Lawsuits by Notice Population Size



51

Incidents disclosed in 2024 resulted in one or more lawsuits filed

(compared to 58 in 2023)

44

Incidents involved SSNs

35

Incidents involved medical/health information

27

Incidents involved a healthcare organization

7

Incidents involved payment card data

32

Incidents involved a network intrusion
23 of these incidents involved ransomware

14

Incidents started with an unpatched vulnerability

2

Incidents were vendor related



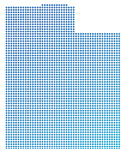
California Invasion of Privacy Act (CIPA) Litigation Is Not Slowing Down

Chasing the enticing possibility of statutory damages continues to drive a flood of class actions related to advertising technology. Claims range from the simple proposition that web technology collects IP addresses in violation of the pen register/trap-and-trace portions of CIPA, to claims that pixels/cookies intercept “communications” (i.e., page views or search terms) while in transit without consent, to more complex conspiracy theories based on allegations that the software code on a website allows third parties to “spy” and build robust profiles of anonymous visitors by matching information like device ID, IP address, and other browsing data. Defendants continue to challenge these novel claims on grounds of personal jurisdiction, standing, and pleading failures, with outcomes largely dependent on the court and the quality of the pleadings.

One of the most significant trends in 2024 was the increased proliferation of trap-and-trace/pen register cases. Although some California courts have dismissed these cases at the pleading stage (see, e.g., *Palacios v. Fandom, Inc.*; *Casillas v. Transitions Optical, Inc. I*; *Casillas v. Traveler’s Choice*; *Licea v. Hickory Farms LLC*; *Levings v. Open Text Corporation*; *Casillas v. Transitions Optical, Inc. II*), there is a lack of uniformity or consistency in decisions due to plaintiffs differing allegations, differing courts and judges, and the variety of issues contested. For example, many of the cases decided in plaintiffs’ favor fail to consider the limiting language of Cal. Penal Code Section 638.51 (making it illegal to “install or use a pen register or trap and trace device without first obtaining a court order pursuant to Section 638.52 or 638.53”) and the practical steps of the court-order process, which require law enforcement to identify a telephone number or telephone line.

Nevertheless, decisions in plaintiffs’ favor, like *Shah v. Fandom, Inc.* (Northern District of California), continue to breathe life into plaintiffs’ novel theories. In *Shah*, the court denied Fandom’s statutory standing challenge and held that the plaintiffs had been “injured” under the statute because they “plausibly alleged” that they were “being tracked across multiple visits for marketing and advertising purposes, and that they did not expect or agree to such tracking.” Although we believe *Shah* is incorrect, that decision and others like it only serve to embolden plaintiffs’ counsel.

To help clients reduce their exposure to these risks, **BakerHostetler is launching a new cookie categorization product** that will leverage our extensive knowledge of third-party tracking technologies to assist with properly classifying cookies under U.S. state privacy laws.



Utah Statute Creates Risk for Disclosing Consumer Data

Utah’s Notice of Intent to Sell Nonpublic Personal Information Act (NISNPIA or the Act) creates notice requirements for commercial entities in Utah, i.e., entities that have “an office or other place of business located in the state,” that disclose their customers’ personal information. NISNPIA awards statutory penalties of \$500 for each violation. Although the Act includes specific language prohibiting class actions, a recent decision from the District of Utah found that because Federal Rule of Civil Procedure 23 does not “abridge, enlarge or modify” substantive rights under the Act, plaintiffs may bring class actions for claims brought under NISNPIA in federal court. *Curry v. Mrs. Fields Gifts, Inc.*; *Arnstein v. Sundance Holdings Grp., LLC*. This issue is currently under consideration in other cases pending in the District of Utah, and we believe that *Curry* and *Arnstein* incorrectly applied the *Shady Grove* choice-of-law analysis. Nevertheless, unless these cases are reversed, we will be watching for increased class litigation against companies in Utah that “disclose” customer information.

Courts Are Still Willing to Dismiss Data Breach Lawsuits for Lack of Standing

Courts dismissing cases for lack of standing was a positive development in 2024. Courts requiring plaintiffs to allege facts that, if proven, would establish that the plaintiffs suffered a concrete injury that is *fairly traceable* to the data breach is critical, especially in light of the concerning trend of expensive settlements. Below are six good examples of cases being dismissed. Perhaps courts are taking notice of the number of these cases and specious harm allegations.



Maser v. Commonspirit Health (District of Colorado) dismissed because an alleged bank fraud was not fairly traceable to the breach despite allegations that the breach resulted in sensitive information being published on the dark web.



In re Samsung Data Sec. Breach Litig. (District of New Jersey) dismissed because the plaintiff could not establish that the specific information obtained in the data breach could not have been obtained elsewhere, e.g., from sources on the dark web unrelated to the data breach.



Stern v. Acad. Mortg. Corp. (District of Utah) dismissed despite allegations of a fraudulent loan made using a plaintiff’s personal information because the plaintiff failed to show traceability between the data breach and the alleged injury.



Williams v. Bienville Orthopaedic Specialists, LLC (Southern District of Mississippi) dismissed despite allegations of actual fraud and data misuse, reasoning that “[d]ata breaches and other forms of data theft are so prevalent that it is seemingly impossible to trace the misuse of personal information to one particular breach[.]”



McGowan v. Core Cashless (Western District of Pennsylvania) dismissed because the plaintiff did not plausibly allege that misuse of her payment card information was imminent despite allegations that “card numbers [are] for sale on the Dark Web whose common purchase point was [defendant].”



Petta v. Christie Business Holding Co., P.C. (Illinois Supreme Court) affirmed dismissal, holding that the alleged harm, an unauthorized loan application, was not fairly traceable to a data breach because the loan application included only publicly available information, such as the plaintiff’s name, phone number, and city and state of residence.

Arbitration: Is It as Good as It Used to Be?

This past year, we saw a spike in individual arbitration demands related to claims, like those under CIPA, that have stiff statutory penalties, e.g., \$5,000 per violation. Although arbitration provisions traditionally were believed to be a business-friendly method to manage the cost, timing, and publicity of litigation, plaintiffs are now using serial or mass arbitration demands as weapons to achieve settlements just below the expected fees and costs associated with initiating arbitration. Plaintiff’s counsel are now identifying a statutory based privacy claim, finding a company with online terms requiring arbitration, collecting thousands of plaintiffs by advertising online, and then sending a demand letter threatening to file arbitration claims on behalf of each person to extract a settlement payment (or face the high cost of arbitration fees if claims are filed).

Given these developments, we recommend analyzing applicable arbitration provisions through this evolving lens, including considering whether existing terms of use:



Govern website interaction or specific transactions



Include provisions to limit mass individual arbitrations



Should include a stand-alone class action waiver

Web Tracking/Pixel Litigation & Regulatory Landscape

Toward the end of 2022, and in the beginning of 2023, we saw an explosion in the number of website privacy lawsuits, particularly against healthcare providers. These new case filings are finally starting to slow down. The big news over the past year on the healthcare front has been favorable. First, the American Hospital Association prevailed in its litigation against the Department of Health and Human Services (HHS) over the government's so-called tracking technologies guidance. *American Hospital Association v. Becerra* (Northern District Texas). Second, the Massachusetts Supreme Judicial Court refused to apply the Commonwealth's wiretap statute — enacted in 1968 — to novel website privacy claims in *Vita v. New England Baptist Hospital*.

The enthusiasm about these victories, however, is tempered by their scope. *The American Hospital Association* decision invalidating HHS's tracking technologies guidance was limited to what the court called the "Proscribed Combination": the alleged disclosure of "an individual's IP address" combined with "a visit to a UPW [unauthenticated public webpage] addressing specific health conditions or healthcare providers." As for *Vita*, unlike federal law, the Massachusetts wiretap statute has not been amended to include provisions specifically with respect to "electronic communications," which was part of the court's rationale for why the statute did not apply. Thus, while both decisions were victories for healthcare providers, we are continuing to advise our clients to exercise caution in their use of digital analytic tools on their public websites.

One reason for this continued caution is shown by *Salazar v. National Basketball Association*. In *Salazar*, the Second Circuit held that the plaintiff was a "subscriber of goods or services" and, therefore, a "consumer" under the federal Video Privacy Protection Act by virtue of providing his email and IP address to the NBA in exchange for a free email newsletter. The Second Circuit rejected the district court's holding that a person must be a subscriber of audiovisual goods or services to be covered by the statute. We have seen an increase in VPPA case filings following *Salazar*.

It remains to be seen whether any other federal circuit courts will follow the Second Circuit's expansive view of the statute. The *Salazar* decision, however, shows how statutes can be interpreted by courts to apply to internet activity that did not exist at the time these statutes were enacted. For website privacy claims against healthcare providers, we are seeing this same phenomenon for statutory claims asserted under the federal Wiretap Act (as amended by the Electronic Communications Privacy Act of 1986), which often survive motions to dismiss.

More broadly, the major development on the litigation side in 2024 has been an increase in the number of website privacy case settlements. This may be a function of the sheer number of cases that were initially filed and some litigation fatigue from the plaintiffs' bar. We are also seeing, however, that many attorneys on the plaintiffs' side are starting to become more reasonable in their assessment of what the cases are worth. This does not apply uniformly across the board, and there are still some parts of the plaintiffs' bar that remain aggressive in valuing and prosecuting website privacy claims, including through the specter of mass arbitration demands and threats.

The major development on the litigation side in 2024 has been an **increase** in the number of **website privacy case settlements**.

Finally, with respect to the regulatory landscape, as in many other contexts, we are waiting to see how things will develop on the healthcare front with the new administration. For HHS's tracking technologies guidance in particular, the department's website continues to state that "HHS is evaluating its next steps in light of [*the American Hospital Association v. Becerra*] order." Thus, whether new guidance will be issued, what that guidance might look like, and whether public notice and comment will be provided this time around all are basic questions that remain to be answered. In recent months, HHS has indicated that including website tracking technologies as part of an organization's HIPAA security risk analysis is required. Additionally, as HHS OCR regroups at the federal level, a few state regulators have ramped up investigations of healthcare websites and the use of tracking technologies under the state's privacy laws and using the state's HIPAA enforcement authority.

OCR/Healthcare

Healthcare cybersecurity and privacy were top of mind for regulators, patients, and threat actors alike in 2024. Health systems again dealt with extortion attempts, hospitals were forced into downtime and pen-and-paper operations for weeks at a time, and countless providers and patients felt the effects of the Change Healthcare breach. The OCR ushered out the prior administration with new HIPAA enforcement initiatives and a flurry of resolution agreements. The federal government implemented and proposed regulations that have a significant impact on healthcare entities — including rules for reproductive health privacy and the FTC Health Breach Notification Rule (see Chapter 13: FTC) as well as proposed rules for HIPAA security and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) impacting critical infrastructure, inclusive of healthcare entities. Some states have signaled a focus on healthcare entities, notably with new regulations in New York with accelerated notification deadlines and attendant settlements with the AG's office. HHS took a significantly activist role under the Biden administration. However, by the end of 2024, many of its hallmark initiatives were successfully challenged, paused, or in litigation — leaving healthcare entities uncertain of what is to come.

2025 is off to another fast start. From major ransomware events to significant policy changes from the new administration, the first quarter is keeping everyone on high alert. We are keeping a watchful eye on the changes occurring in the new administration. Cybersecurity has proven to be a bipartisan issue, and we feel confident it will continue to be top of mind as the new administration sets its agenda.

Change Healthcare Ransomware Attack

We represented
125
 organizations
 in responding
 to the Change
 Healthcare
 incident.

The ransomware attack on Change Healthcare in February 2024 not only impacted the operations and payment for services of thousands of healthcare providers and health plans but it also reportedly affected the PHI of over 190 million Americans. Change brought to light the interconnected relationship of healthcare vendors and the systemic impact when a cybersecurity incident affects one of those vendors. Over a year later, Change continued to notify affected patients and health plan members. Healthcare organizations learned that their vendor contracts, including business associate agreements, may be with a company different from the one with which they originally contracted. Additionally, some of those contracts and business associate agreements went back decades, and the business associate provisions were not favorable to the providers. The Change incident received a great deal of attention and scrutiny from HHS, which has prompted action in the form of new proposed rules and guidance for ransomware and other cybersecurity incidents. Vendor incidents have consistently plagued our healthcare clients over the past decade, and it is common that when a vendor in this industry reports an incident, it impacts multiple providers and other covered entities.

Reproductive Health Privacy

The HIPAA Final Rule to Support Reproductive Health Privacy focused on preventing access to PHI for individuals who seek, provide, and receive lawful healthcare services related to their reproductive system. While the definition of reproductive healthcare is broad and does not mention abortion or transgender care specifically, the commentary expressly stated that the final rule is in response to patients' and providers' confidentiality concerns in the wake of *Dobbs*. The rule is now effective for HIPAA-regulated entities.

HIPAA-covered entities and business associates struggled with implementing the rule, given the extent to which they regularly share information with governmental entities that, in turn, have been largely unwilling to comply with and/or are unaware of the processes required before even routine PHI disclosures.

Numerous legal actions were filed regarding the final rule, politicizing the regulation, demonstrating the burden on healthcare entities and the desire to protect this sensitive information. Even with the pending litigation, the new administration may choose to not enforce the rule or to conduct new rulemaking to roll back these protections. The uncertainty — which includes the possibility of a reversal in direction after the midterm elections or with a new administration in four years — created by all of this activity will likely continue.

Increased Focus on Security

Healthcare organizations, as critical infrastructure, found themselves subject to the provisions of CIRCIA. Though enacted in 2022, the Cybersecurity and Infrastructure Security Agency (CISA) did not issue its Notice of Proposed Rule Making (NPRM) until April 2024. CIRCIA applies to entities within the healthcare and public health sectors and includes hospitals of 100 beds or more, critical access hospitals, essential medicine manufacturers, and Class II and III device manufacturers. Under CIRCIA, an entity would be required to report certain cyber incidents and ransom payments to CISA within 72 hours of becoming aware of the incident, create detailed incident reports, and preserve incident-related evidence. These requirements are more stringent than HIPAA and could create regulatory activity arising from the reporting of these cross-agency communications.

In late December 2024, approximately 50 HIPAA-regulated entities received audit requests from the OCR focused on HIPAA Security Rule compliance with 30 days to respond. While the audits were voluntary, the OCR indicated that a compliance investigation could result from the response — or perhaps the lack thereof. Additionally, HHS issued an NPRM with significant proposed changes to the Security Rule in late December. These changes include a 72-hour recovery period following a cyber incident, written security risk analysis and risk management plans with specific parameters, new requirements for business associates, and numerous other additions and changes to HIPAA's existing security provisions. With the change in administration, there remains significant uncertainty about the NPRM's viability.

HIPAA Enforcement Activity

The OCR's enforcement activity got off to a slow start in 2024, but picked up by Q4. Overall, the OCR has announced a total of 22 enforcement actions that its resolved in 2024, including six resolution agreements for Right of Access. The remaining enforcement actions demonstrate the OCR's continued focus on:



Security Risk Analysis Initiative: The OCR announced four resolutions under a newly announced Risk Analysis Initiative. These matters were resolved in less than half of OCR's normal timeline. HIPAA's requirement for entities to conduct a comprehensive, enterprise-wide security risk analysis (SRA) has consistently been a focus of the OCR in enforcement actions. The agency will either critique an SRA for not being adequate or critique the covered entity for not mitigating a risk identified in the SRA. With the addition of the cybersecurity practice goals and the eight newly proposed requirements in the HIPAA Security Rule NPRM, we anticipate that the SRA will remain a key point in the new administration.



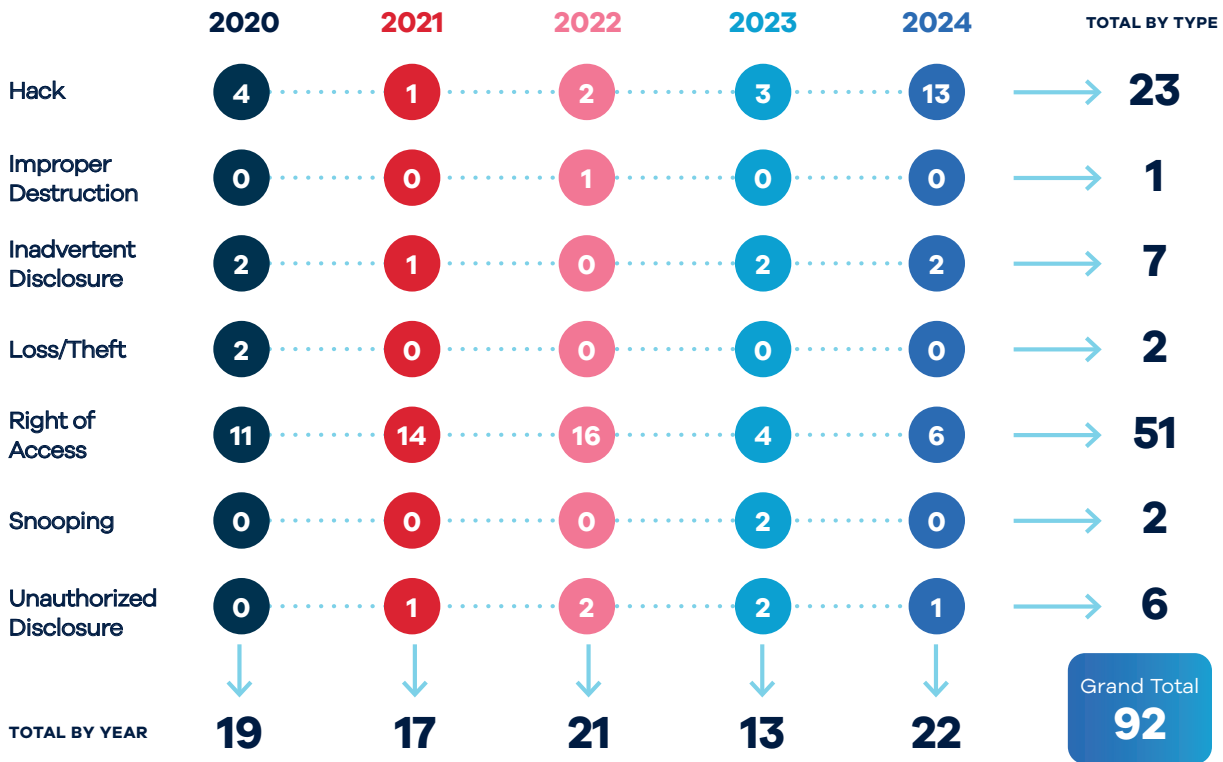
Ransomware: In our last report, we discussed the first-ever ransomware-related resolution agreement and anticipated there would be more to come. Jump to 2024, and eight of the resolutions reached arose from ransomware investigations. Ransomware attacks prove to be extremely costly to healthcare organizations due to downtime, ransom payments, and resulting class actions. The OCR showed it is not swayed by entities' victim status and will use the attack to conduct a detailed HIPAA compliance audit, adding to the overall cost of the attack.



Business Associates: Between 2015 and 2020, the OCR reached resolutions with only four business associates. In the past two years, the OCR increased its enforcement activity with business associates, demonstrating the OCR's recognition of the role business associates play in the healthcare industry and the agency's commitment to enforcing compliance of the business associates. This activity, though, creates, in some instances, protracted negotiations between covered entities and business associates as they try to limit their exposure and liability through business associate agreements.

Ransomware attacks prove to be **extremely costly to healthcare organizations** due to downtime, ransom payments, and resulting class actions.

OCR Enforcement Tracker



Based on Resolution Agreements/Notices of Final Determination announced as of March 2025, grouped by year of settlement/final determination.

From the first enforcement action in 2008 to the end of 2024:

164

(22 in 2024)

Cases settled, or that imposed a civil monetary penalty

\$16M

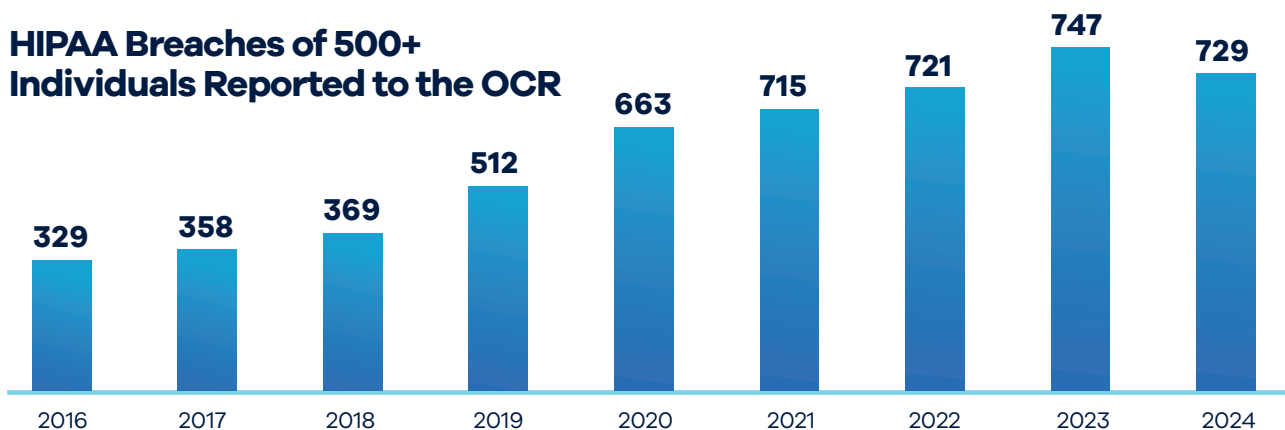
(\$3M in 2024)

Highest amount paid as part of a resolution agreement

\$157.3M

(\$9.9M in 2024)

Amount collected by the OCR through its enforcement actions



Securities & Exchange Commission

Companies entered 2024 concerned about the ability to comply with the Securities and Exchange Commission (SEC) cybersecurity rules, which fell into two categories: (1) cybersecurity strategy disclosure (Form 10-K Item 1C) and (2) materiality (Form 8-K Item 1.05). The four-day timeline to file an 8-K upon determining materiality was the biggest concern. A year later, the landscape looks a lot different, and the level of concern is much lower.

Cybersecurity Strategy and Governance Disclosures

Many companies were concerned that the new obligation to disclose a company's cybersecurity risk management strategy would create "gotcha" moments that would lead to increased regulatory scrutiny and litigation when the company disclosed a security incident that suggested that something about the company's cybersecurity strategy disclosure was not accurate. However, most companies thoughtfully made disclosures describing security methods and process (not implementation or efficacy), so we did not see this risk materialize.

Fewer than

1%

of our matters for public companies involved a decision to file an 8-K Item 1.05

Material Cybersecurity Incidents

Similar to the first year after the GDPR went into effect, when companies were over-notifying regulators, 2024 started with companies filing 8-Ks even though the companies had not determined that the incidents were material. All of the first 18 disclosures filed under Item 1.05 of Form 8-K stated that the company was still assessing whether the impact on the financial condition or operations was material. None mentioned qualitative factor impacts. So, the SEC issued guidance on May 21, 2024, recommending that companies not file under Item 1.05 unless the company had determined that the cybersecurity incident was material. For incidents where the impact was not yet known or was not material but the company wanted to disclose the incident in a filing, the SEC encouraged companies to instead use Item 8.01.

In total, companies filed 26 initial Form 8-K Item 1.05 disclosures from December 2023 through December 2024. It was not until the 26th one — filed on December 11, 2024, by a restaurant company for an incident that disrupted its online ordering — that a filing stated that the incident had a material impact on the company's operations and financial condition.

Indeed, material cybersecurity incidents are rare. In 2024, fewer than 1% of our matters for public companies involved an 8-K filing.

One ransomware group attempted to use the 8-K requirement as additional extortion pressure by filing a whistleblower report with the SEC after the company did not pay a ransom and did not file a Form 8-K. The attempt drew media coverage but likely did not have the impact the ransomware group hoped it would have.

SEC Enforcement

SEC enforcement actions that were active in litigation or resolved in 2024 arose from incidents that occurred before the effective date of the cybersecurity rules, and they were almost exclusively related to the 2020 SolarWinds incident. The civil fraud lawsuit brought by the SEC against SolarWinds and its CISO was the most notable action, and the July 2024 ruling dismissing many of the claims was regarded as a stinging defeat for the SEC.

Shareholder Litigation

Although the frequency of lawsuits by consumers against a company after disclosure of a security incident has increased over the past five years, securities and governance class actions and shareholder derivative claims are rare. Of the 26 companies that filed a Form 8-K Item 1.05 regarding a cybersecurity incident in 2024, only two faced a shareholder lawsuit (and one lawsuit was withdrawn). The shareholder derivative claims filed were for breach of fiduciary duty, indemnification, contribution, and violations of Sections 14(a) and 20(a) of the Exchange Act.

What to Expect in 2025

Under the new administration, we expect to see more decisions in line with Republican commissioners' dissents from 2024 and — potentially — fewer enforcement actions (e.g., dissents specifically took issue with the SEC's use of Section 13(b)(2)(B)'s internal accounting controls provision as a Swiss Army knife to compel companies to implement cybersecurity policies and procedures the SEC thinks prudent in the absence of explicit requirements to do so).

Take Action: Here are three governance actions to take:

1

Impact Assessment Process — Verify that there is an internal protocol and process for:

- detecting cybersecurity incidents;
- classifying incidents by potential impact (e.g., low, medium, high, critical);
- escalating incidents based on severity classification to a committee that evaluates disclosure obligations (e.g., escalate all high and critical incidents);
- assessing impact based on applicable qualitative and quantitative factors;
- determining and documenting the decision regarding the impact assessment; and
- if applicable, filing a Form 8-K under Item 1.05 or 8.01.

Doing an executive tabletop exercise is an effective way to test and refine this process and protocol. Having members of the audit committee or board observe the exercise or briefing them on the exercise is a good way to enable effective oversight.

2

Bringdown Process

Ensure that there is a process to review statements related to cybersecurity before quarterly and annual filings for accuracy and completeness, including based on any security incidents or assessments that occurred since the prior filing and to avoid hypothetical statements regarding actual risks that have occurred.

3

Security Statements

Review public-facing security statements for accuracy, completeness, and consistency.

Global Privacy

Data transfers between Europe and the United States have long been mired in uncertainty and bureaucracy. In 2025, we expect data transfers to be back in the spotlight due to the convergence of international AI competition, privacy and data protection concerns, fragmented cross-border transfer approaches, and geopolitical dynamics. Countries are increasingly considering protectionist measures, such as data localization and residency requirements, particularly with respect to critical infrastructure and national security but also for financial, health, and telecommunications data — and even business records.

In the European Union, the hard-won EU-U.S. Data Privacy Framework adequacy decision, which permits freer transfers of personal data for certified companies, is under renewed U.S. scrutiny due to initiatives by the new administration to strengthen U.S. surveillance while simultaneously reducing independent oversight. The Court of Justice of the European Union recently ruled that plaintiffs can receive compensation for nonmaterial damages resulting from unlawful personal data transfers. Although the amount awarded was minimal (a little over \$400) in this particular case, the decision could lead to more challenges and possibly collective actions regarding personal data transfers from the EU. Additionally, the Data Act, which received less attention in the United States than other EU digital strategy legislation did, will facilitate data sharing within Europe while complicating extra-European data transfers, dragging nonpersonal and even proprietary business data into the transatlantic transfer miasma.

While attention predominantly has been focused on transatlantic data-transfer hiccups, other countries have been developing their own transfer restrictions, localization requirements, and attendant spools of red tape. For example, the Association of Southeast Asian Nations and the Latin American Data Protection Board have created model clauses for personal data transfers. Individual countries, including Brazil, China, New Zealand, and the United Kingdom, also have developed their own models. However, model clauses are just one mechanism for personal data transfers. Other countries require consent, approvals, security assessments, or registrations, and some simply prohibit certain transfers outright. Over the past year, several multimillion-dollar fines have been imposed by regulators, including in South Korea for personal data transfers without consent, in Sweden for failures to implement suitable adtech settings to prevent personal data transfers, and in the Netherlands for not implementing lawful personal data transfer mechanisms.

Last but certainly not least, the United States has begun adding complexity to cross-border data flows, potentially disrupting outbound data flows from the country. Executive Order 14117, issued in 2024, was implemented through DOJ rulemaking and security requirements from CISA and finalized just before the new administration took office. This rule and the requirements restrict transfers of Americans' bulk sensitive data, broadly defined, to designated countries of concern and impose additional security requirements to prevent these same countries from accessing the data. At the time of rulemaking, the designated countries were limited to China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela. However, should the new administration retain this framework, additional countries could easily be added. New laws, such as the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA), place further restrictions on the transfer of data outside the United States. Although these new U.S. restrictions target data brokers, the definitions of data broker adopted are broader than many companies might expect. Anticipate more refinement of the U.S. stance on transfers as the new administration seeks to embrace more protectionist policies. Given that data has become the most valuable commodity, other types of trade restrictions could significantly impact data uses and transfers.

Take Action

It is essential for companies to understand the origins of their data and which laws apply to it. With increasingly complex data flows, it's rarely as simple as assuming that a company based in one country will be subject to only that country's laws. For example, if companies wait until a security incident occurs to determine what countries' laws apply to the affected data, they risk having to disclose the incident to regulators despite their data processing being noncompliant with applicable laws. Additionally, making beneficial use of the data (e.g., for internal analytics), developing AI tools, and other data monetization methods may be nearly impossible if the company has not established the right to use the data for the intended purpose. Businesses should bear in mind that access is often considered a type of data transfer. Finally, anticipate that data transfer restrictions may change rapidly, monitor developments, and have contingency plans in place.

State Comprehensive Privacy Laws

New State Privacy Laws Took Effect

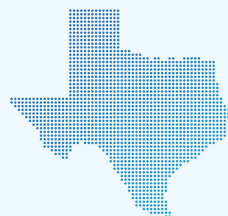
With the failure of yet another attempt at a comprehensive federal privacy law, privacy regulation in the United States remains primarily a matter of state law. However, the absence of a federal law should in no way be interpreted as evidence of any lack of interest in the U.S. regarding regulating the collection, processing, and disclosure of personal data. In 2024, new comprehensive privacy laws took effect in Texas, Oregon, and Montana, bringing the total number of covered states to eight and the total percentage of covered consumers to 34%. These statistics do not include the Florida Digital Bill of Rights (due to its relatively narrow applicability) or the Washington My Health My Data Act and Nevada SB370 (due to their narrow focus on consumer health data), although all three of these laws also took effect in 2024.

Within the patchwork of state privacy laws, we continue to see similar rights and requirements relating to notices, opt-outs, contracts, and the rights to access, delete, and correct personal data. On the other hand, 2024 also saw the introduction of novel features, including the Oregon law's right to obtain a list of third parties to which a controller discloses personal data and the Texas law's explicit notice requirements for sales of sensitive data and biometric data. The Texas law also introduced a novel test for applicability that does not depend on the volume of personal data a business collects but instead turns on whether a company does business in the state or produces products or services consumed by state residents and does not qualify as a "small business" under the standards maintained by the U.S. Small Business Administration (SBA). Other states, including Minnesota and Nebraska, subsequently incorporated reference to the SBA standards into their privacy laws, which take effect in 2025.

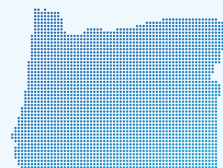
Whether or not Congress again takes up federal privacy legislation in 2025, the wave of new state laws shows no sign of slowing down. By the end of the year, eight more state privacy laws will be in effect. And even in states without a comprehensive privacy law, we will continue to see guidance and enforcement on privacy issues, as exemplified by the New York Attorney General's guidance on website privacy issued in July 2024.

In 2024, new comprehensive privacy laws took effect in Texas, Oregon, and Montana, bringing the total number of regulated states to **eight** and the total percentage of covered consumers to

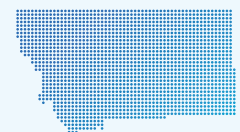
34%



Texas



Oregon



Montana



California



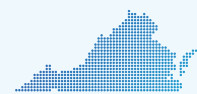
Colorado



Connecticut



Utah

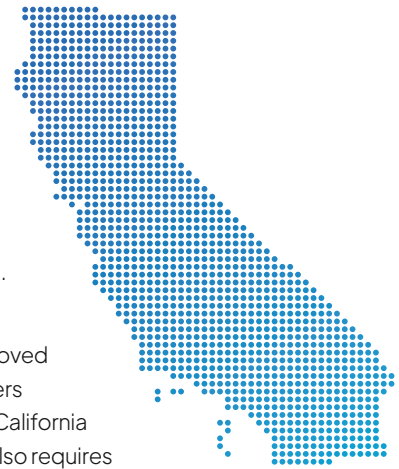


Virginia

All Eyes on California – Updates to Rulemaking and Other Developments

California privacy laws and regulations continue to be in flux, requiring businesses to stay on alert to adapt to new or evolving requirements. Further amendments to the California Consumer Privacy Act (CCPA) that clarify the inclusion of neural data as a sensitive category, among other changes, are in effect. The much-anticipated updated CCPA regulations are still working their way through the public comment process, with the California Privacy Protection Agency (CPPA) commencing formal rulemaking in late 2024, including sections on Cybersecurity Audits, Privacy Risk Assessments, and the controversial Automated Decisionmaking Technologies (ADMTs) in the draft regulations. These draft regulations will take effect and be enforceable immediately upon approval, which could be as early as summer 2025.

Meanwhile, California's 2023 Delete Act amended its existing data broker registration law, which places oversight of data brokers under the CPPA. In addition, in November 2024, the CPPA approved new regulations to implement the Delete Act, which increased the registration fee for data brokers and expanded the definition of "direct relationship." By 2026, the CPPA must create a portal for California residents to make opt-out and deletion requests to all registered data brokers. The Delete Act also requires data brokers to register, pay fees, and disclose information about various topics, such as consumer requests, children's data, and sensitive personal data.

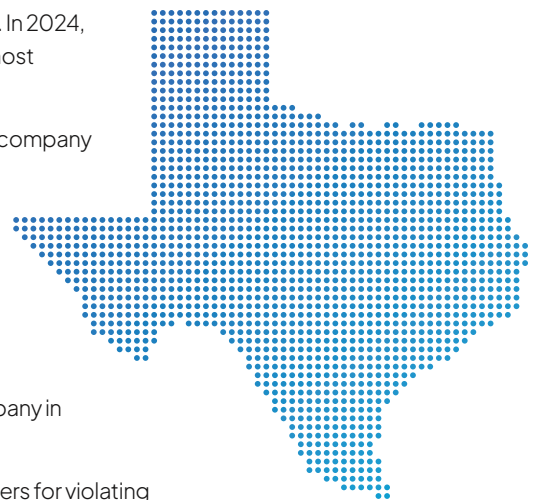


Is Everything Bigger in Texas? U.S. State Privacy Enforcement in 2024

Against the backdrop of ongoing privacy enforcement actions at the federal level, the states continued to ramp up privacy enforcement of their own, with Texas leading the way. In 2024, the Lone Star State donned boots and spurs, demonstrating its reputation as the most aggressive state privacy regulator in the United States.

The Texas Attorney General concluded a significant settlement with a social media company relating to biometric data, launched investigations into the automotive industry for alleged surveillance and data sharing practices, issued notices to over 100 companies for failing to comply with the Texas data broker law, and began a lawsuit and a large-scale probe into companies for suspected violations of the Securing Children Online through Parental Empowerment (SCOPE) Act and the Texas Data Privacy and Security Act. At the beginning of 2025, the Texas Attorney General became notable for bringing the first lawsuit against a company in alleged violation of a comprehensive state privacy law in its case against an insurance company in relation to its geolocation data sharing practices.

To the west, in California, the CPPA announced a settlement with multiple data brokers for violating the Delete Act and devoted other efforts to staffing up its Enforcement and Audit teams. The CPPA also published two enforcement advisories relating to dark patterns and data minimization as they relate to consumer requests. California's other enforcer of the CCPA, the Attorney General, signaled its focus on children's data through a joint settlement with the Los Angeles city attorney against a mobile app developer for violations of both the CCPA and the Children's Online Privacy Protection Act (COPPA). Earlier in the year, the Attorney General announced a settlement with a food delivery service company also for violating the CCPA and COPPA.



Information Governance

In 2024, the SEC and the Commodity Futures Trading Commission (CFTC) continued their interest in how regulated organizations maintain books and records according to federal securities law requirements, many of which require such be kept in a non-rewritable, non-erasable format (also known as “write once, read many,” which has one of the best acronyms in information governance — WORM).

Specifically, between August and September 2024 (continuing a slate of enforcement stretching several years) the SEC and CFTC announced over \$478 million in fines against 37 firms registered as broker dealers and/or investment advisers. Per the SEC, each of its investigations “uncovered pervasive and longstanding use of unapproved communication methods, known as off-channel communications” (e.g., via WhatsApp or text). The firms admitted “their personnel sent and received off-channel communications that were records required to be maintained under the securities laws. The failure to maintain and preserve required records deprives the SEC of these communications in its investigations. The failures involved personnel at multiple levels of authority, including supervisors and senior managers.” Also in September, the SEC announced \$49 million in fines against six credit rating agencies for failing to maintain and preserve electronic communications.

In addition to monetary penalties, several of the firms were also required to retain compliance consultants to, among other things, conduct comprehensive reviews of applicable policies and procedures and help improve risk management activities. Notably, the SEC highlighted that proactive efforts to address compliance failures will pay off — one additional firm was not required to pay a penalty at all because it “self-reported, self-policed, and demonstrated substantial efforts at compliance,” and the penalties imposed on other firms were less than they would have been because of, in part, their early efforts to comply with subject recordkeeping requirements. Perhaps the early (proactive) bird does get the worm (get it?).

Striking a balance between fostering a secure and responsible environment and meeting record retention requirements or needs can seem daunting. Whether your organization is subject to a strict set of recordkeeping requirements or the incident response statistics related to data theft provided earlier in this report justifiably frighten you — your organization’s Information Governance Program should be a top priority. Taking action should include the following:

- Mapping out the current state of your communications systems and document retention processes to identify areas that need to be addressed and to outline your desired future state.
- Drafting new or revising existing policies and procedures to describe (and accurately reflect) your Information Governance Program.
- Implementing these policies and procedures across the organization and testing their effectiveness.

Between August and September 2024, the SEC and CFTC issued over

\$478M in fines to 37 firms

for failing to maintain required records — highlighting that proactive compliance efforts can significantly reduce penalties or even eliminate them entirely.

Federal Trade Commission

Junk Fees (The FTC's Version)

In December 2024, the FTC announced a bipartisan rule, the Junk Fees Rule, banning so-called junk fees. Though not in time for Swifties and the Eras Tour, the rule, effective May 12, 2025, prohibits the “bait-and-switch” pricing for live-event tickets and hotel stays. According to the FTC, these practices are unfair and deceptive and “undercut honest businesses.” The Junk Fees Rule requires that businesses disclose the true total price, inclusive of all mandatory fees, when they offer, display, or advertise any price of live-event tickets or short-term lodging and that the total price be displayed more prominently than any other pricing information. This means that truthful itemization and breakdowns are fine but should not overshadow what consumers want to know: the real total.

Finalized Updates to COPPA

In January 2025, the FTC announced finalized amendments to COPPA, concluding a process first kicked off in early 2024 when its Notice of Proposed Rulemaking was issued. Once effective, website operators will need to obtain opt-in, verifiable consent from parents before disclosing children’s data to third parties, including for behavioral/targeted advertising purposes. Additionally, a website operator may not cut off a child’s access to the site if a parent refuses to consent to disclosure, and behavioral advertising must be off by default for users under thirteen. Other notable amendments include limiting the retention of children’s data and expanding the definition of “personal information” to include biometric identifiers.

The COPPA amendments will become effective 60 days after being published in the Federal Register. Under the new administration, it may be some time before the COPPA amendments are published.

Health Breach Notification Final Rule

The FTC vastly expanded both the types of companies that are covered by its breach notification rule and the types of disclosures that would trigger the new notification provisions. The FTC estimated that the rule, which went into effect on July 29, 2024, would apply to at least 193,000 entities (that includes only non-HIPAA-covered entities that collect and maintain consumer health information). Unlike HIPAA, where, for the most part, violations occur when PHI is either stolen by or unintentionally disclosed to unauthorized third parties, the FTC’s rule would be triggered by intentional disclosures of health information if the consumers, based on the posted privacy policies, would not have expected their information to be used in that way. Although the FTC previously indicated that it would be watching for and pursuing health applications that do not adequately describe data-sharing programs, it did not publicly announce enforcement of this rule in 2024.



The FTC’s Junk Fees Rule bans hidden fees in live-event tickets and hotel stays, requiring businesses to disclose the full price upfront — no more surprises at checkout.

Looking Ahead:



Ferguson Takes Over

In January 2025, Republican Commissioner Andrew Ferguson took over as FTC Chair after nearly four years with Lina Khan at the helm. Under Ferguson, we can expect to see a more targeted approach to privacy and technology, particularly the collection of sensitive data, with a focus on clearer violations of existing law, less rulemaking, and continued enforcement.



“Cop on the Beat” Enforcement

We expect to see more FTC focus on traditional law enforcement and less on creative or novel “unfairness” theories of liability. Ferguson has expressed concerns about the FTC attempting to regulate targeted advertising and AI, for example, suggesting that the agency will focus on using the clear authority it has rather than pursuing companies under novel theories of existing law.



New Rules, New Focus

The FTC likely will seek to enforce new rules that have bipartisan support, including the Imposter Rule, the Junk Fees Rule, and the Rule on Consumer Reviews and Testimonials.



What Else?

We also may see some agency activity regarding social media platforms and compliance with terms of service and issues relating to content moderation, as well as increased interest in self-regulatory programs such as the BBB National Programs of the National Advertising Division.



Join us for the next episode of BakerHosts™ AD Nauseam, a podcast series focusing on new and trending advertising issues with an emphasis on the FTC and the NAD.

www.bakerlaw.com/podcasts/ad-nauseam/

CHAPTER 14

Digital Assets

A new era for digital assets is upon us. On January 21, 2025, the SEC launched a crypto task force, led by Commissioner Hester Peirce, “dedicated to developing a comprehensive and clear regulatory framework for crypto assets.” Shortly thereafter, on January 23, President Trump signed an Executive Order, “Strengthening American Leadership in Digital Financial Technology,” which “supports the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy.” The Commission is implementing the directive expeditiously. For example, it rescinded the controversial Staff Accounting Bulletin (SAB) 121, which required entities holding their customers’ crypto assets to record those as liabilities on their balance sheets, replacing it with SAB 122, which applies accounting principles for contingent liabilities. More pro-digital asset policies are expected to emerge as President Trump aims to fulfill his campaign promise to make the U.S. the “crypto capital of the planet.”

With this new national policy, the digital asset economy finds itself on the precipice of unprecedented opportunities. As innovation accelerates, digital assets are poised to revolutionize industries, change financial landscapes, and open the door to new business models.

In December 2024, **BakerHostetler launched the Digital and Innovative Markets Team** — a revolutionary legal marketplace offering designed to seamlessly integrate traditional financial markets and the rapidly evolving digital markets by providing cohesive, forward-thinking legal and strategic advice on the digital, capital, and commodities and derivatives markets.

Digital Asset Types and Use Cases

Below are some of the most popular use cases for digital assets:



Payment

Leveraging blockchain for decentralization and security, assets can be traded 24/7 globally.



Functional

Assets that enable access to an application, good, or service.



Commodity

They represent commodities (agricultural goods and rights) and are traded on a futures market.



Security

Assets that represent a security, investment, or ownership.



Asset-Backed Stablecoin

Often tied to fiat currency, they can minimize price volatility.



Tokenized Real-World Assets

A token of a real-world asset (e.g., commodities, real estate, finance) allowing fractional trading.



Non-Fungible Tokens (NFTs)

Unique tokens often used for art, collectibles, and other one-of-a-kind items to verify ownership and authenticity. They can also be tickets and support loyalty programs.



Hybrid

Digital assets may combine the characteristics of more than one classification.

Artificial Intelligence

2024 was a banner year for AI law, regulation, and guidance, and the news told the tale...

Europeans First Out of the Gate

The European Union Artificial Intelligence Act (EU AI Act) was approved by EU member countries in February 2024; it was then approved by the European Parliament on March 13, 2024, and became law on May 21, 2024, when the Council of the EU announced its final approval. The EU AI Act was introduced as the central pillar of policy measures aimed at supporting the development of trustworthy AI. It also included an AI Innovation Package and the Coordinated Plan on AI. For Europeans and participants in the EU market, that full EU AI Act package focused on several core elements that became themes in the United States as well, specifically:



Scope and Enforcement of AI Violations



A Risk-Based Approach to AI



Prohibited and High-Risk AI Systems



General-Purpose AI Models and Generative AI

U.S. Federal Guidance

On this side of the Atlantic, also in February 2024, the then-deputy U.S. Attorney General provided guidance on how the DOJ planned to govern — and punish improper uses of — AI, including how the DOJ considered self-policing government use of AI and what that might mean for DOJ practices generally. In December 2024, bookending the year, the CFTC issued its own non-binding AI compliance obligations in an advisory on the “Use of Artificial Intelligence in CFTC-Regulated Markets,” providing a non-exhaustive list of existing statutory and regulatory requirements that CFTC-regulated entities’ use of AI might implicate.

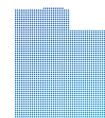
CHAPTER 15: ARTIFICIAL INTELLIGENCE

U.S. State Laws and Regulations



March — Oct 2024 | California: CCPA's Overview of Proposed Revisions to CCPA

Attempts to clarify what an ADMT is (technology that “executes a decision, replaces human decisionmaking, or substantially facilitates human decisionmaking”); what an ADMT is not; and what Risk Assessments will look like. In April 2025, following the public comment period, the CCPA Board scaled back the proposed regulations. Specifically, the Board removed requirements that restricted the use of personal data for targeted advertising and AI training, tapered certain definitions (and thus the overall scope of the proposed rules), and cut back on businesses’ documentation requirements.



May 2024 | Utah Artificial Intelligence Policy Act (UAIPA)

Utah became the first state to enact an AI-centric consumer protection law. The UAIPA enforces the mandates first outlined in March 2024 regarding the disclosure and accountability of generative AI use in customer communications. Organizations regulated by Utah’s Department of Commerce (*i.e.*, those that require a license or state certification) must actively and prominently disclose to consumers (before any interaction occurs) that Gen AI is used. The UAIPA requires all other organizations subject to Utah’s consumer protection laws to passively disclose any use of Gen AI in a “clear and conspicuous” manner. Under the UAIPA, companies are responsible for the Gen AI output; in effect, they view statements made by a Gen AI tool as if they were said by an actual employee of the company. Notably, the UAIPA also created the Office of Artificial Intelligence Policy, which is tasked, in part, with creating and administering an AI Learning Lab Program, focused on AI development and innovation.



August 2024 | Colorado's AI Act

The Act will apply to high-risk uses of AI affecting Colorado “consumers,” defined as all Colorado residents — meaning, unlike with most privacy laws, there are no employment or business-to-business exceptions (but there are limited carve-outs for existing laws and some industries). Colorado’s AI Act will not take effect until February 1, 2026.



August 2024 | Illinois: the Limit Predictive Analytics Use Bill

The Bill, which goes into effect on January 1, 2026, amends the Illinois Human Rights Act to prohibit certain uses of AI by employers as well as to outline notice requirements.

U.S. State Regulator Guidance

Other industry bodies, noting both activity and delays at the U.S. federal and state levels, took matters into their own hands.

A March 2024 bulletin posted by the Illinois Department of Insurance reflected on how the National Association of Insurance Commissioners had promulgated a 2023 Model Bulletin on AI that was expected to be incorporated at the state level. In July 2024, the New York Department of Financial Services (NYDFS) released its Circular Letter No. 7, “Use of Artificial Intelligence Systems and External Consumer Data and Information Sources in Insurance Underwriting and Pricing,” which was directed to (among others) all insurers authorized to write insurance in New York state. The Circular Letter provides guidance on the insurance industry’s disclosure and transparency obligations, as well as governance and documentation expectations related to the use of AI. The NYDFS also published an industry letter in October 2024 in response to “inquiries about how AI is changing cyber risk and how Covered Entities can mitigate risks associated with AI.” That letter outlined four specific risks associated with AI: (1) AI-enabled social engineering; (2) AI-enhanced cybersecurity attacks; (3) exposure or theft of vast amounts of nonpublic information; and (4) increased vulnerabilities due to third-party, vendor, and other supply chain dependencies.

It Takes a Village to Make a Patchwork

Taking everything proposed in 2024 into account presents less of a picture and more of a framework in which some companies have struggled to find certainty. The organization that fits neatly into any one framework is rare indeed; this multiplicity of approaches and staggered guidance and implementation dates made it challenging for multinational organizations to stay compliant or even abreast of current and future requirements. This was especially difficult when, for example, Utah’s AIPA went into immediate effect, but the Colorado AI Act, while slated for 2026 implementation, was still subject to further potential changes. Perhaps that is the most solid takeaway from 2024 AI learnings: The one constant going forward will be change.

To receive an electronic version of this report, please visit bakerlaw.com/DSIR.

BakerHostetler is a leading law firm recognized for client service that helps organizations around the world address their most complex and critical business and regulatory issues.

Our Digital Assets and Data Management (DADM) Practice Group is a convergence practice addressing enterprise risks, disputes, compliance, and opportunities through the life cycle of data, technology, advertising, and innovation, including brand strategies and monetization. We have united key service offerings and technologists to address all the risks associated with an entity's digital assets. Our clients are collecting data and then utilizing advanced technology to transform their products and services. Doing this creates enterprise risk. We work with our clients through the life cycle of data — privacy, security, marketing and advertising, transactions, and emerging technology.

Chair, DADM Practice Group

Theodore J. Kobus III
New York
T +1.212.271.1504
tkobus@bakerlaw.com

Editors in Chief

Ryan M. Christian Sr.
Atlanta
T +1.404.256.8234
rchristian@bakerlaw.com

Elise R. Elam
Cincinnati
T +1.513.929.3490
eelam@bakerlaw.com

Kimberly C. Gordy
Houston
T +1.713.646.1360
kgordy@bakerlaw.com

Courtney L. Litchfield
Chicago
T +1.312.416.6236
clitchfield@bakerlaw.com

DADM PRACTICE GROUP TEAMS

Digital Risk Advisory and Cybersecurity

Craig A. Hoffman
Cincinnati
T +1.513.929.3491
cahoffman@bakerlaw.com

Andreas T. Kaltsounis
Seattle
T +1.206.566.7080
akaltsounis@bakerlaw.com

Advertising, Marketing and Digital Media

Amy Ralph Mudge
Washington, D.C.
T +1.202.861.1519
amudge@bakerlaw.com

Privacy Governance and Technology Transactions

Janine Anthony Bowen
Atlanta
T +1.404.946.9816
jbowen@bakerlaw.com

Melinda L. McLellan
New York
T +1.212.589.4679
mmclellan@bakerlaw.com

Healthcare Privacy and Compliance

Lynn Sessions
Houston
T +1.713.646.1352
lsessions@bakerlaw.com

Privacy and Digital Risk Class Action and Litigation

Paul G. Karlsgodt
Denver
T +1.303.764.4013
pkarlsgodt@bakerlaw.com

Emerging Technology

Katherine Lowry
CIO and Head of IncuBaker
Cincinnati
T +1.513.852.2631
klowry@bakerlaw.com

James A. Sherer
New York
T +1.212.589.4279
jsherer@bakerlaw.com

Digital Transformation and Data Economy

Janine Anthony Bowen
Atlanta
T +1.404.946.9816
jbowen@bakerlaw.com

Chad A. Rutkowski
Philadelphia
T +1.215.564.8910
crutkowski@bakerlaw.com

Digital and Innovative Markets

Teresa Goody Guillén
Washington, D.C.
T +1.202.861.1360
tgoodyguillen@bakerlaw.com

BakerHostetler

bakerlaw.com

v2

© 2025 BakerHostetler