BakerHostetler

2023 DATA SECURITY INCIDENT RESPONSE REPORT

Reassess & Recalibrate

Security Measures & Approach

FEATURING INSIGHTS FROM **DIGITAL ASSETS AND DATA MANAGEMENT** GROUP TEAMS

DSIR 2023

Key Findings

Threat Actors Adapt.

Organizations have strengthened security measures and become more resilient, but threat actors are still finding ways through. MFA bombing, social engineering, EDR-evading malware, sophisticated credential stuffing techniques – you name it, they're trying it.

But the More Things Change, the More They Stay the Same.

Network intrusions were still the most common type of incident, and threat actors typically gain access in the same old ways – phishing, unpatched vulnerabilities, etc.

MFAiled.

You've implemented MFA, but Bob in Accounting inadvertently approved the MFA prompt. Good controls can be defeated by untrained (and trained) employees.

On Again, Off Again - And On Again.

Most ransomware groups may have been busy doing something else in early 2022, but they returned with a vengeance at the end of the year and into 2023.

Key IR Metrics Improve.

Companies are getting quicker at identifying – and containing – network intrusions. Preparation counts.

Average Ransom Paid Increased.

After three years of increasing average amounts followed by a decrease in the average ransom paid in 2021, we saw a 15% increase in 2022.

Forensic Investigation Costs Increased, Too.

By 20% on average in network intrusion matters, which does not include business interruption costs, data review and notice costs, indemnity claims, etc.

The Long Road to Recovery.

The average time to recover after a ransomware incident increased across all industries. Do you have a business continuity plan, and have you tested it in production?

Don't Be a Hoarder.

Please. We've asked so nicely before. Get rid of your old data. No one wants to notify decades of former employees and regulators are asking questions about the age of data involved in incidents.

Post Data Breach Lawsuit Filings More Prolific.

Lawsuits are being filed more frequently after a data breach incident is disclosed. And they are being filed in smaller matters (fewer than 10,000 individuals affected).

Uncle Sam Gains Ground on Ransomware.

Law enforcement attacked the ransomware issue by imposing sanctions on groups (Conti), groups that facilitated initial network access (Trickbot operators), and a service that protected payments (the Blender.io virtual currency mixer). Additional measures were used to disrupt groups that drew attention (Hive).

BECs on the Decline?

Despite years of business email compromises leading to fraudulent wire transfers (and years of guidance on how to avoid them), BECs surged in 2021. In 2022, the overall number and dollar value of fraudulent transfers decreased from the prior year.

It's Not Just California Anymore.

Four other states enacted privacy legislation in 2022, and one more just announced legislation in 2023. Are you taking a holistic approach to compliance?

Don't Sleep on Compliance – Regulators Aren't.

In Europe and elsewhere, there has been a rise in investigations into organizations' privacy compliance programs unprompted by a breach notification. Get your privacy compliance house in order before a regulator comes knocking.

Is That a Pixel in Your Eye?

Or is it just on your webpage? Pixel litigation has surged. Ensure you know what website technologies are in place and why.

DeFi and SDLC.

With some of the largest crypto thefts in 2022 resulting from code-related issues, the software development life cycle is more important than ever: companies in this space should be sure to adopt – and follow – a secure coding process to lower the likelihood of significant hacks and thefts.

Table of Contents

CHAPTER 01

Clients & Friends of the Firm

Welcome to our 9th annual Data Security Incident Response Report!

We are now three years post pandemic, and while a lot has changed, some things remain the same. Last year, I talked about resilience—the uncertainties of the pandemic were still present, the war in Ukraine had just begun, and businesses were addressing new issues caused by technology evolution and work-pattern changes. Resilience in 2022 meant continued effective implementation of security measures, evolving privacy compliance programs beyond just addressing the biggest compliance risk areas, and responding to continued efforts by litigators to exploit different privacy and privacy-adjacent statutes for financial gain.

The "incident response boom" in 2020 to 2021 saw new vendor entrants to the market. Some of those vendors were suddenly desperate for work in light of the rapid decrease in network intrusions and ransomware incidents. That lull was short-lived. The attacks picked up at the end of 2022 and have continued into 2023.

Over the past 20 years, our attorneys have spent a lot of time on-site with our clients helping them manage security incidents. That experience gave us a window into how our clients interacted with the life cycle of data and technology. We learned our clients' business, industry, and what mattered from a practical perspective. In 2020, we did something no other law firm has done—we elevated data issues to the practice group level (similar to tax, IP, litigation, labor and employment, and business). The group is called Digital Assets and Data Management (DADM). In the three short years we have been in existence as a firm practice group (rather than a practice team), we are approaching the size of our firm's IP group, have more than 100 dedicated attorneys and technologists, and have several clients using the services of all seven practice teams. *The American Lawyer*, Chambers, Legal 500, and BTI continue to recognize our accomplishments.

Data issues are cross-practice issues. For example, clients are talking to us about leveraging an existing security tool for privacy management and governance, risk, and compliance (GRC). That type of engagement involves our incident response attorneys, our in-house legal technology team (IncuBaker), and our privacy compliance attorneys. Our adtech, privacy transaction, and privacy attorneys join to help clients manage the sprint to launch new products and services and to build compliance programs for multi-state and global privacy laws. Our litigators responded to the surge of new lawsuits based on security incidents and allegations of violations of privacy laws. Our regulatory, healthcare, advertising, and security attorneys (combined with corporate compliance attorneys) worked to address the federal regulatory focus on cybersecurity, dark patterns, crypto, and post-*Dobbs* issues. You will see insights and guidance based on this work in this year's DSIR report.

I remain proud of the efforts of our firm and the DADM group leading the way on DEI efforts. BakerHostetler achieved Mansfield 5.0 certification this past fall. The leader of our IncuBaker team was named the CIO of our firm, and her team continues to receive accolades for their use of technology in serving clients. We remain the most diverse practice group at BakerHostetler.

Thank you to our clients and the vendors we partner with for all of your support. We hope you enjoy this edition of the DSIR Report, and we welcome you to contact our DADM group members with questions or suggestions.

Sincerely,

Ted Kobus
(He, Him, His) | Chair, Digital Assets and Data Management Group

1,160+
incidents in 2022

U.S. Breach Notification Law Interactive Map
bakerlaw.com/BreachNotificationLawMap

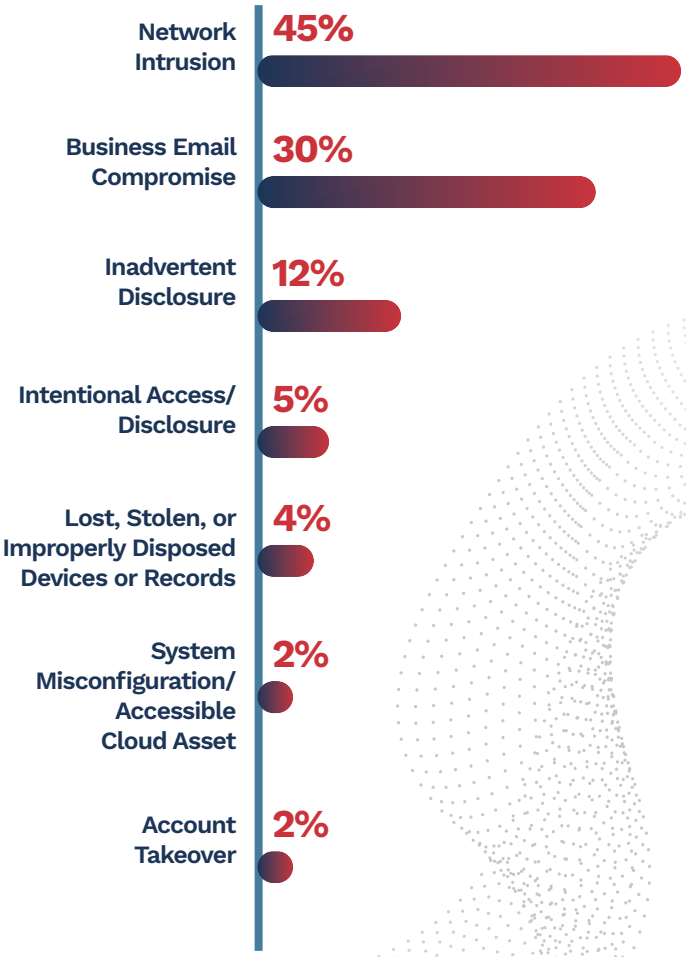
EU GDPR Data Breach Notification Resource Map
bakerlaw.com/EUGDPRResourceMap

CHAPTER 02

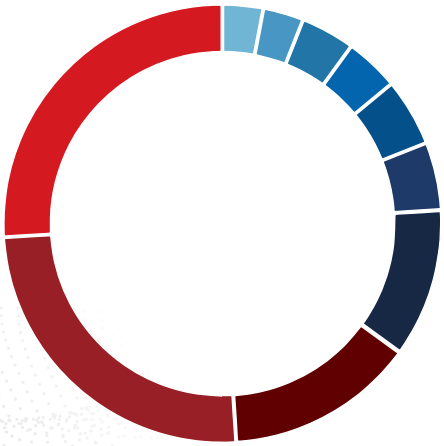
Incident Response Trends

At a Glance

Incident Type



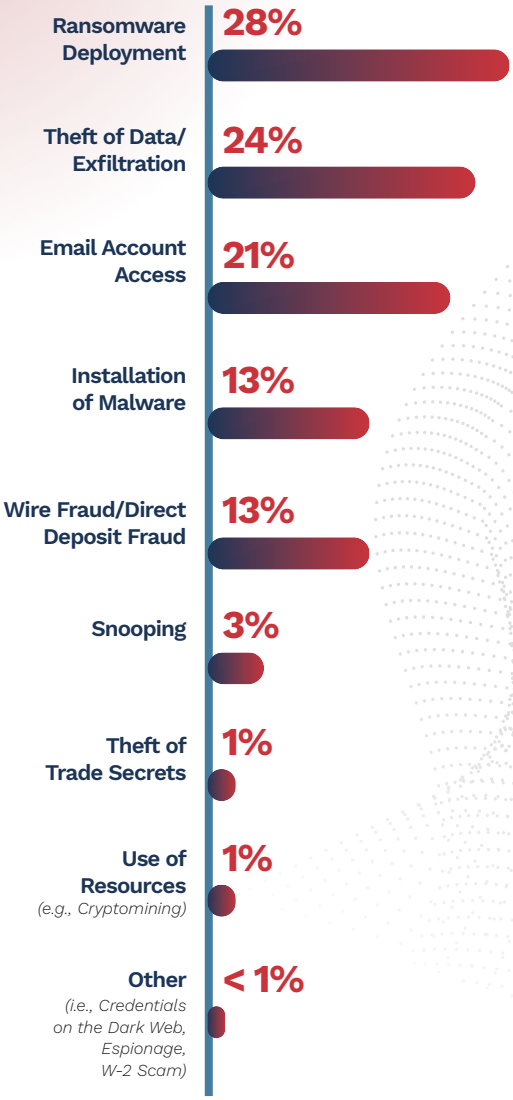
Root Cause



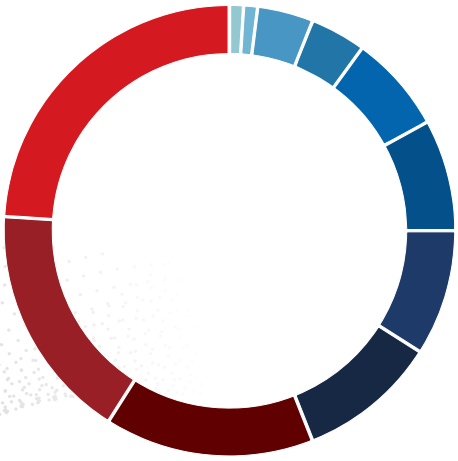
- 26% Root Cause Unknown
- 25% Phishing
- 14% Other *(e.g., Pixel, Device Theft, Skimmers)*
- 11% Unpatched Vulnerability
- 5% Social Engineering
- 5% Other Human Error *(e.g., Unintended Recipient)*
- 4% Misconfiguration
- 4% Employee Abuse of Access Privileges
- 3% Open RDP
- 3% Brute Force/ Credential Stuffing

While business email compromises increased in 2022, fraudulent wire transfers decreased. Moreover, the frequency of network intrusions decreased until the end of 2022, when we saw a dramatic increase, primarily due to an uptick in ransomware.

What Happens After Access



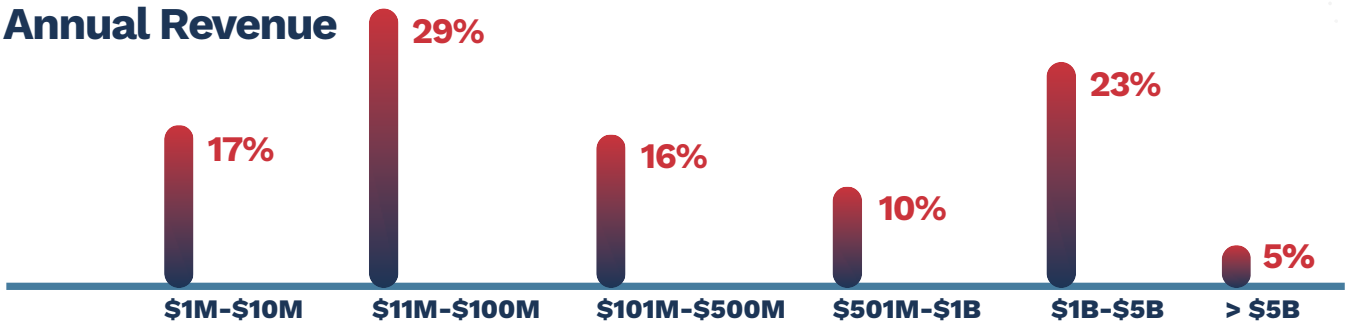
Industries Affected



- 24% Healthcare *(including Biotech & Pharma)*
- 17% Finance & Insurance
- 15% Business & Professional Services *(including Engineering, Transportation, and Managed Service Providers)*
- 10% Retail, Restaurant, & Hospitality *(including Media & Entertainment)*
- 9% Education
- 8% Manufacturing
- 7% Government
- 4% Technology
- 4% Non-Profit
- 1% Energy
- 1% Other

16% of our 1,160+ matters involved vendor incidents.

Entity Size by Annual Revenue



Incident Response Timeline *(Median)*

3 DAYS — From Occurrence to Discovery

0 DAYS — Discovery to Containment

24 DAYS — Time to Complete Forensic Investigation

67 DAYS — Discovery to Notification

Notifications vs. Lawsuits & Regulatory Inquiries

494 Notifications *(44% of matters)*

153 Regulatory Inquiries

42 Lawsuits Filed

47,851 Average Number of Individuals Notified

Average Forensic Investigation Costs

$58,009
All Incidents

$550,987
20 Largest Network Intrusion Incidents

$90,335
Network Intrusion Incidents

Average Ransom Demand & Payment

$3,713,939
Ransom Demand

$600,688
Ransom Payment

Wire Fraud

$27 Million
Total Amount of Fraudulent Wire Transfers

$294,137
Average Wire Transfer

$97,044
Median Wire Transfer

$7.6 Million
Largest Wire Transfer

24%
Matters that Recovered Funds
(totaling over $14.25 Million)

$648,060
Average Recovery

$92,043
Median Recovery

CHAPTER 03

Industries Affected

**Data is listed in averages unless otherwise noted*

Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
FINANCE & INSURANCE				
$5,441,758 (median: $650,000)	**$546,250** (median: $287,500)	**8.9** (median: 1)	**$33,280** (median: $14,000)	**99,154** (median: 498)
MANUFACTURING				
$5,154,765 (median: $1,420,000)	**$402,273** (median: $275,000)	**11** (median: 7)	**$50,638** (median: $42,120)	**5,941** (median: 372)
BUSINESS & PROFESSIONAL SERVICES				
$4,340,967 (median: $350,000)	**$509,412** (median: $155,688)	**13.9** (median: 9)	**$35,522** (median: $23,800)	**29,172** (median: 225)
ENERGY & TECHNOLOGY				
$3,833,064 (median: $1,300,000)	**$386,800** (median: $322,000)	**7.1** (median: 6.5)	**$124,587** (median: $43,000)	**5,828** (median: 714)
HEALTHCARE				
$3,257,688 (median: $1,475,000)	**$1,562,141** (median: $500,000)	**10.3** (median: 7)	**$73,781** (median: $30,000)	**71,370** (median: 696)
RETAIL, RESTAURANT, & HOSPITALITY				
$2,924,938 (median: $1,460,000)	**$555,000** (median: $225,000)	**14.9** (median: 12)	**$48,280** (median: $39,000)	**35,945** (median: 1,322)
EDUCATION				
$1,791,650 (median: $750,000)	**$281,525** (median: $175,000)	**12** (median: 7)	**$68,695** (median: $53,000)	**9,567** (median: 415)
GOVERNMENT				
$1,069,120 (median: $500,000)	**$101,500** (median: $68,000)	**16.8** (median: 8)	**$100,293** (median: $23,750)	**19,701** (median: 2,004)
NON-PROFIT				
$261,500 (median: $261,500)	**N/A** (median: N/A)	**18.3** (median: 15)	**$21,708** (median: $16,500)	**3,073** (median: 1,329)

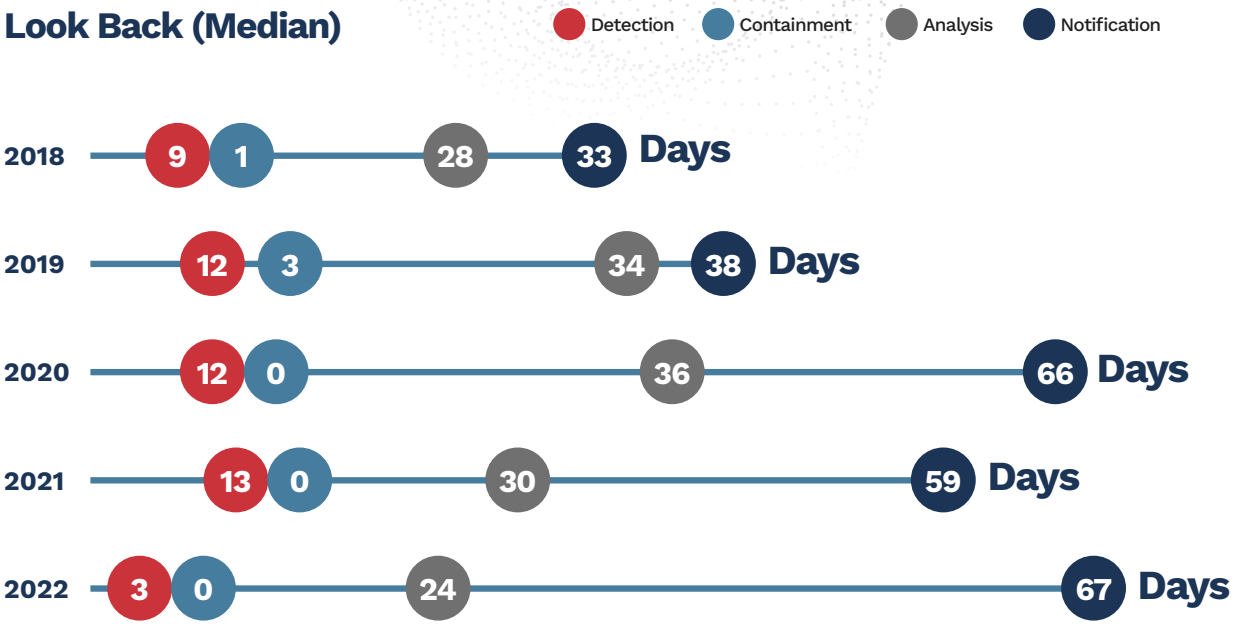
CHAPTER 04

Incident Response Life Cycle

Incident Response Timeline

	Detection Occurrence to Discovery	Containment Discovery to Containment	Analysis Time to Complete Forensic Investigation	Notification Discovery to Notification
Median	**3** Days	**0** Days	**24** Days	**67** Days
Average All Incidents	**63** Days	**4** Days	**31** Days	**83** Days
Average Network Intrusion	**39** Days	**3** Days	**36** Days	**80** Days

Incident Response Timeline Look Back (Median)



CHAPTER 05

Deeper Dive into the Data

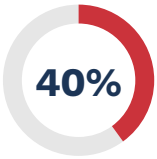
Largest Ransom Demand in 2022:
$90+ million
($60+ million in 2021)

Largest Ransom Paid in 2022:
$8+ million
($5.5 million in 2021)

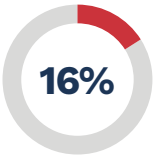
Average Ransom Paid in 2022:
$600,688
($511,957 in 2021)

Ransomware Timeline

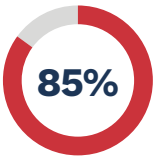
Year	Demand to Payment	Demand to Payment for Payments <$1M	Demand to Payment for Payments > $1M	Encryption to Restoration
2020 Average	8 Days	7.4 Days	9.2 Days	13 Days
2021 Average	11.1 Days	13 Days	9.8 Days	12.2 Days
2022 Average	14.2 Days	14 Days	14.9 Days	12.7 Days
2022 Median	11 Days	11 Days	15 Days	8 Days



of organizations paid a ransom

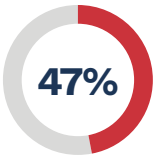


paid even though the organization was able to fully restore from backups

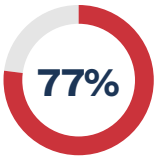


of the time an organization was able to partially or fully restore from backup without paying ransom

found evidence of data exfiltration when there was a claim of data theft in the ransom note



paid even though the organization was able to partially restore from backups



involved theft of data resulting in notice to individuals

Forensic Trends

The multi-year trend of improvement on key incident response metrics continued. In network intrusion matters, dwell time dropped from 66 days to 39 days due to enhanced network visibility (EDR, MDR, SIEM) and ransomware groups completing their mission in less than a day (the time from first access to awareness when encryption occurs is short). The reduction in average time to contain (down from four days to three) may be attributed to companies using the "kill switch" (containment by shutting the system off) more often. Greater prevalence of EDR usage pre-incident, as well as forensic firms being "tool agnostic" and using triage collection scripts, enables quicker investigations (36 days to completion, down from 41 days).

The news is not all positive – the average time to recover from a ransomware incident increased in almost every industry. One reason may be that companies suffering ransomware attacks now are less mature than prior victims.

Comparing Timelines for Network Intrusion Incidents with and without an EDR tool:

Take Action: Be Resilient.

TO BE MORE RESILIENT, COMPANIES CAN:

- **Segment their networks**
- **Use widely deployed and properly configured security tools** that are monitored 24/7 by internal or external security operations centers and that have the anti-uninstall feature enabled
- **Ensure that all critical systems are backed up using immutable backups**
- **Identify a list of critical applications and the order of precedence for restoration**
- **Ensure their business continuity plans identify manual workarounds** that companies can use in the event key systems are encrypted
- **Conduct cross-functional training and testing exercises** that involve activation of all teams in the Business Continuity/Disaster Recovery Plan

Ransomware Is Back in Full Force

After several years of threat actors using an attack method, you expect herd immunity to develop after enough companies enact effective measures. The implementation of P2PE mostly ended card present payment card attacks. We thought MFA might do the same for email account access incidents (not yet). Ransomware began to emerge in 2018 (our average ransom paid was $28,000 then). After five years, widespread immunity is not in sight. Wide deployment of an effective EDR tool that is set to high enforcement mode with active monitoring and the anti-uninstall feature enabled is the primary differentiator between companies that get encrypted and those that do not. Even if you do not stop the data theft/encryption combo from occurring, having available backups to restore from reduces the overall impact.

As the number of vulnerable companies in the herd thins (because they improved on their own, they improved after suffering a ransomware attack, or they improved to get through underwriting for cyber insurance), the remaining may be even more vulnerable. In 2022, we saw increases in average ransom demands, average ransom payments, and average recovery times in most industries. The lull in ransomware that marked the start of the year is over. Ransomware groups have resumed attacks, and organizations must redouble their efforts to defend themselves against increasing attacks.

A Slow Start but a Strong Finish

Ransomware matters slowed in the first half of 2022, with many attributing the slowdown to the war between Russia and Ukraine. Ransomware returned with a vengeance near the end of the year, however, and is only continuing to increase in pace in 2023.

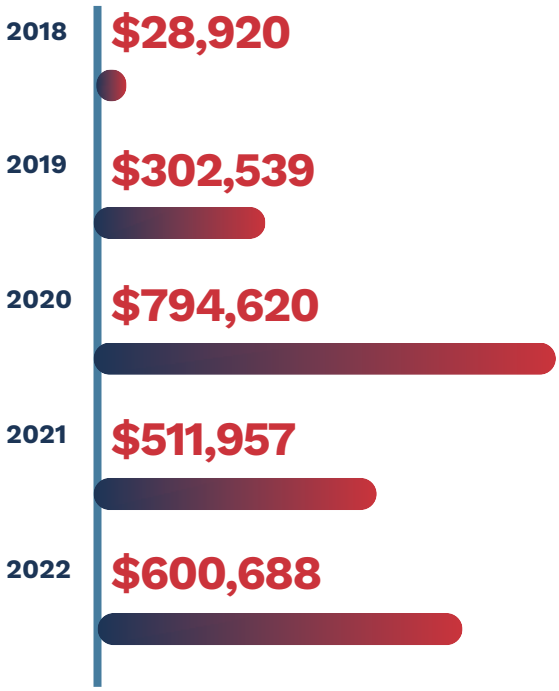
Recovery Times Increase Significantly

The average time to recover from a ransomware incident extended in almost every industry and, in most cases, significantly. Average recovery times in some industries were over a week longer than in 2021. The retail, restaurant and hospitality industry was particularly hard hit, with average recovery times increasing from 7.8 days in 2021 to 14.9 days in 2022 – a 91% increase. However, they weren't alone: the healthcare; energy and technology; and government industry segments also saw notable increases, at 69%, 54%, and 46%, respectively.

Ransom Demands and Payments Increase

Average ransom demands and payments increased in 2022. The average ransom demand increased in six of the eight industries we tracked.

AVERAGE RANSOM PAYMENT:



Forensic Investigation Costs Showed More Variation

Three industries — finance and insurance; business and professional services; and retail, restaurant, and hospitality — showed decreases in both the average and median costs as compared to 2021. Two industries — government and energy and technology — saw higher averages but lower medians, reflecting a general decrease in costs for most clients but offset by some significant ransomware matters for certain clients. Two other industries — healthcare and manufacturing — saw increases in both the average and median amounts spent on forensic investigations in 2022. The average forensic investigation costs for the 20 largest network intrusion incidents increased 24% over 2021, growing from $445,926 to $550,987.

Successful Fraudulent Fund Transfers Continue to Decrease

We spent an entire page covering fraudulent transfers in our report last year due to their prevalence. In 2022, every metric we track for fraudulent fund transfers showed a decrease. We saw fewer transfers. The total amount of transfers and average transfer amount were down:

TOTAL AMOUNT OF TRANSFERS

$48 million in 2021

$27 million in 2022

AVERAGE TRANSFER AMOUNT

$743,106 in 2021

$294,137 in 2022

LARGEST WIRE TRANSFER

$12 million in 2021

$7.6 million in 2022

All of these figures are moving in the right direction. A discouraging development, however, is that the percentage of matters in which funds were recovered and the amounts recovered decreased.

MATTERS WITH RECOVERED FUNDS

42% in 2021

24% in 2022

AVERAGE RECOVERY

$890,135 in 2021

$648,060 in 2022

MEDIAN RECOVERY

$181,577 in 2021

$92,043 in 2022

CHAPTER 06

Threat Actors Adapt

Finding New Ways Around Security Measures

Organizations responded to the ransomware epidemic seriously, deploying a host of security measures that were far less common a few years ago than they are today. Multi-factor authentication (MFA) for email and remote access; endpoint detection and response (EDR) tools; patch management solutions; security incident and event management tools; immutable backups; and internal and third-party security operations centers to monitor host and network activity in real time — these solutions have been implemented with increasing frequency to combat the methods threat actors most commonly use to gain access to networks and enhance the ability to recover. Punch, counterpunch. The threat actors responded in kind, finding new ways to evade the measures that organizations put into place. A few of the tactics we observed in 2022 are:

MFA Bombing

After gaining an account's username and password, threat actors repeatedly attempt to authenticate, which presents the employee with MFA requests. Employees sometimes acquiesce, hitting "Approve," and the threat actor is in. Identifying more effective methods for authentication and training employees remains important.

Social Engineering

Threat actors continue to use social engineering, where they impersonate a customer, a member of the IT team, or some other trusted source in conversations with an organization's employee. One group is notoriously effective. In some cases, these communications occur over months, with the threat actor gathering more information about the target over time; they then use that information to convince an employee to take some action, such as providing their credentials, approving a request to connect to the employee's device, or providing confidential information about an organization's customers. Technical safeguards are important, and so are administrative safeguards (*e.g.*, employee training).

Evading EDR

While not common, some groups have developed methods to evade EDR tools. One example is the use of polymorphic malware like Qakbot. Exploiting "coverage deficits," where the agent was not installed on all assets, is the more common method of "evading" an EDR tool. Asset management, comprehensive EDR deployment, proper EDR configuration, and 24/7 monitoring to detect follow-on activity are important.

SEO Poisoning

We also saw threat actors create fraudulent websites that mimicked a client's legitimate website and then use search engine optimization tactics to make the fraudulent website show up prominently in search results. The website includes a sign-in feature, where deceived individuals would enter their credentials. The threat actor then uses the credentials to log into the customer's account and perform unauthorized activity, such as making unauthorized purchases, creating new users, or exporting data. These incidents can be difficult to detect and combat, but there are service providers that can assist with responding to them.

CHAPTER 07

Data Privacy Litigation Trends

1,160+
Incidents Handled in 2022

494
Incidents with Notification

42
Incidents with Notification Resulted in One or More Lawsuits Filed

Lawsuits by Notice Population Size

< 1,000
People Notified:
4 Lawsuits

101k - 500K
People Notified:
13 Lawsuits

1,001 to 10,000
People Notified:
2 Lawsuits

501k - 1M
People Notified:
2 Lawsuits

10,001 to 100K
People Notified:
12 Lawsuits

< 1M
People Notified:
9 Lawsuits

Lawsuits nearly doubled year over year. No longer are only the 'big breaches' capturing attention.

42
Incidents disclosed in 2022 resulted in one or more lawsuits filed
(compared to 23 in 2021)

40
Incidents involved SSNs and/or DL#s

26
Incidents involved medical/health information

6
Incidents involved payment card data

20
Incidents involved a healthcare organization

36
Incidents involved a network intrusion

11
Incidents started with an unpatched vulnerability

10
Incidents were vendor related

Privacy Statute Litigation Is on the Rise

CALIFORNIA INVASION OF PRIVACY ACT (CIPA) LITIGATION

Beginning in June 2022, a wave of class action lawsuits hit California retailers and consumer-facing service providers alleging violations of alleging violations of CIPA. The lawsuits claim defendants permitted third-party vendors to unlawfully eavesdrop on customers' communications made through the defendants' online chat feature. The sudden surge of cases began with the Ninth Circuit's unpublished decision in *Javier v. Assurance IQ*, which held CIPA "applies to Internet communications." Relying on *Javier*, several "creative" plaintiff's firms have circulated hundreds (if not thousands) of pre-suit demand letters threatening CIPA class litigation under two provisions of CIPA statutes—§ 631(a) and § 632.7. Over 100 cases have been filed in state and federal courts throughout California.

Fortunately, there have been numerous motions to dismiss granted in federal court, and they provide a solid framework for attacking these CIPA "chat-bot" wiretapping cases, including:

- The § 631 aiding and abetting prong only applies when the alleged third party's actions and use of the data are wholly independent of the website owner and not undertaken at the direction of, or for the benefit of, the website owner;
- Plaintiffs are unable to allege sufficient facts demonstrating the chat communications were "intercepted" while "in transit" as opposed to being collected or recorded after the fact; and
- § 632.7 only applies to communications between a cellular radio or cordless telephone on one side and a cellular radio or cordless or landline telephone on the other side. Because the retailer is not using an applicable telephone device to communicate, § 632.7 cannot apply.

VIDEO PRIVACY PROTECTION ACT (VPPA) LITIGATION

Congress passed the VPPA (18 U.S.C. § 2710(b)) in 1998 to address video rental privacy concerns after Blockbuster disclosed a U.S. Supreme Court nominee's video rental history to a news outlet. In 2012, the VPPA was updated to cover digital streaming and on-demand services. The VPPA prohibits any videotape service provider (VTSP) from knowingly disclosing, to any person, personally identifiable information concerning the VTSP's consumer. Violators face a maximum $2,500 penalty per class member.

Recent cases are surviving motions to dismiss in the website tracking context even when the website tracks a user through a Meta Pixel or other software and provides videos incidental to its actual business purpose. In one case, the court denied the defendant's motion to dismiss because the plaintiff had plausibly pled that he subscribed to goods and services from a VTSP – *USA Today* – under the VPPA. *See Belozerov v. Gannett Co*. In another, the motion to dismiss was *denied* in a putative class action where the plaintiffs alleged that the Boston Globe disclosed personally identifiable information of subscribers to Facebook in violation of the VPPA. *See Ambrose v. Boston Globe Media Partners LLC*. Finally, a motion to dismiss was denied in another putative class action where it was alleged that the NFL app violates the VPPA because it shares Android phone users' pre-recorded video requests, as opposed to the viewing of live footage, with Google's marketing apparatus. *See Louth v. NFL Enterprises LLC*.

Key defenses are still being litigated in the VPPA context, including:

- The defendant is not *engaged* in the business of rental, sale, or delivery of prerecorded video cassette tapes or *similar audio-visual* materials;
- The defendant is unaware of what information the website tracker is collecting;
- For providers of free video content, the plaintiff is not a "renter, purchaser, or subscriber of goods or services" from the VTSP; and
- The defendant provided the plaintiff informed consent in a distinct and separate form.

RIGHT OF PUBLICITY STATUTES

Class action filings alleging that any type of "sharing" of a consumer's data violates states' publicity or misappropriation statutes are on the rise. Notable examples of those statutes include:

- Illinois' Right of Publicity Act (IRPA) ($1,000 per violation)
- California's Right of Publicity Law (CRPL) ($750 per violation)
- South Dakota's Right of Publicity Law (SDRPL) ($1,000 to $3,000 per violation)
- Ohio's Right of Publicity Law (ORPL) ($2,500 to $10,000 per violation)
- Puerto Rico's Right of Publicity Act (PRRPA) ($750 to $20,000 per violation)

Fortunately, the majority of these cases are not surviving motions to dismiss. For example, in both *Huston v. Hearst Communications, Inc.* and *Farris v. The Orvis Co.*, the courts dismissed the matter, holding (1) plaintiff's identity is, itself, the product and is not being used to promote some other product, which is necessary to state a claim; and (2) the mere mention of plaintiff's name in sold mailing lists did not constitute an appropriation of plaintiff's personality. However, further litigation on these statutes is anticipated. Despite these defendant-favorable rulings, a few cases have proceeded past motions to dismiss.

ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

More than 1,700 BIPA class actions have been filed since late 2017, with no signs of slowing down. BIPA provides for a private right of action with liquidated statutory damages of $1,000 for each negligent violation and $5,000 for each reckless or intentional violation, plus attorneys' fees and costs.

On October 12, 2022, the first BIPA case proceeded to a trial, and the jury returned a judgment of $228 million on a class of 45,600 truckers who had scanned their fingers to gain access to a railroad terminal (*i.e.,* $5,000 per class member). In February 2023, the Illinois Supreme Court issued two decisions holding that the BIPA statute of limitations is five years for all claims and such statute of limitations accrues with each scan or transmission of biometric data. Per-person demands are increasing, as is the filing of BIPA-related lawsuits.

Class Certification in Data Breach Litigation Remains Uncertain

Lawsuits are being filed more often after security incidents are disclosed. However, the plaintiff's has suffered defeats at the class certification phase.

In October 2022, the Court of Appeal of the State of California affirmed the denial of class certification to individuals asserting claims under California's Confidentiality of Medical Information Act (CMIA) based on their patient and medical data being stolen by a former employee. Specifically, the court held that a breach of confidentiality under CMIA is an "individualized issue" and in this case would require individualized inquiries into "whether third parties used plaintiffs' information, whether this use was without authorization, the timing of this misuse, whether plaintiffs took measures to protect against the misuse of their information, whether the information used was involved in the data breach, and whether third parties could have obtained this information through other means." This is a big win for healthcare defendants, and also a pivotal leverage point for all privacy class certification litigation in California.

In addition, a district court in California denied class certification to individuals whose personal information was stolen in a data breach because the named plaintiff (and anyone who signed the defendant's terms of use) waived any right to represent the class or subclass based on the "class action and jury trial waiver" provision in defendant's terms of use. Despite litigating the action for nearly two years, the court determined that the defendant had not waived its right to enforce this provision because the affirmative defense was raised in its answer. The ruling is another important win for California defendants and a reminder that classaction waiver provisions and affirmative defenses can still be valuable business tools.

There are two key appellate cases where classes were certified in data breach cases involving a hospitality company and a restaurant group. We will be watching both cases closely in 2023.

CHAPTER 8

Pixel & Other Website Technologies Take Center Stage

The *Dobbs* decision coincided with the publication of an investigative report about the use of advertising technology on hospital websites. Several regulators scrambled to give consumers, health apps, and HIPAA-covered entities admonishments and guidance on the risks and limitations surrounding the use of this type of technology. Simultaneously, a deluge of class actions was filed, alleging various causes of action stemming from the use of this technology. For many healthcare entities, 2022 will be remembered as "The Year of the Pixel."

A Tidal Wave of Proactive Regulatory Activity

Regulators got involved quickly after the *Dobbs* decision and the aforementioned article was published:

HHS OCR issued guidance asserting that consumers should understand many menstrual cycle and health tracking apps are not subject to HIPAA and information provided to those app providers by consumers is not subject to the regulation's protections.

The FTC warned they would investigate health technology companies if they mislead consumers about data anonymization or data sharing.

HHS OCR guidance asserted that if HIPAA-covered entities are sending IP addresses of website visitors to tracking technology vendors, then these IP addresses are PHI. Accordingly, a business associate agreement must be in place or the covered entity needs to assess the disclosure under the breach risk assessment standard. We have worked with dozens of clients regarding this issue and believe there are opportunities to determine no breach occurred.

HHS OCR, state attorneys general, and U.S. Congress members issued dozens of investigation demands to health industry entities related to the use of tracking technology on websites.

The focus on website technologies and health-related information is likely to continue in 2023 and beyond. Entities should ensure a strong corporate governance process and collaborative approach between marketing and compliance departments, an in-depth understanding of the use of this technology, and a thorough assessment of the risks and benefits conferred on the entity to determine whether continued use is appropriate.

The FTC Reminds Health-Tech That the OCR Is Not the Only Health Entity Regulator

In February and March 2023, the FTC announced a $1.5 million settlement with a prescription coupon service and a $7.8 million settlement with a mental health provider in two matters that appear to have been in the works within the FTC since well before July 2022. In both cases, the FTC challenged health entities sharing consumer health data with third parties for advertising purposes. After several quiet years in the health technology industry, the sudden uptick in the FTC's activity is likely due to the perfect storm of a post-*Dobbs* era, where online activity could be used against consumers, and the throng of health-tech startups coming to market in the last few years, driven, at least in part, by needs newly identified during COVID. Non-HIPAA-regulated entities need to take a very close look at their privacy policies, ensure that all third-party sharing is adequately described, and ensure that they are obtaining express consent from consumers for any sharing of health information, particularly if the sharing is related to advertising.

A New Wave of Privacy Class Actions

Since August 2022, more than 50 lawsuits have been filed against hospital systems, alleging they track and disclose patients' identities and online activities via third-party website analytics tools without the website visitors' knowledge and consent. The claims asserted include those based on (a) contracts (alleged inaccurate website privacy policies or notices); (b) state privacy laws (alleged unauthorized disclosures of personal and/or health information to third parties); and (c) federal or state wiretapping laws (alleged interceptions of communications). Motion to dismiss briefing is ongoing in many of these cases and involves these issues:

- **Breach of contract:** Whether HIPAA-required privacy notices form a contract and plaintiffs' failure to allege specific contract provisions allegedly breached.
- **State privacy laws:** Whether plaintiffs consented to the alleged tracking and plaintiffs' failure to state facts showing a "highly offensive" intrusion.
- **Breach of confidence, negligence, and breach of fiduciary duty:** Whether a state already has a common law tort for the alleged unauthorized disclosure.
- **State consumer protection laws:** Whether the plaintiff has identified sufficient damages.

In addition to determining whether any of these arguments would be appropriate in a motion to dismiss, defendants should consider the following:

- For wiretap act claims, evaluate whether "contents" of communications are at issue, and whether the statute requires two- or one-party consent, as the latter may foreclose the occurrence of "interception."
- Evaluate whether claims are subject to binding arbitration and/or class action waivers, which may form the basis of a successful motion to compel arbitration or a motion to strike class allegations, respectively.

If claims survive a motion to dismiss, opposing class certification becomes critical. Entities should focus on key differences in putative class members' experiences to narrow a class (purpose for visiting website, pages visited, and browser and device settings – each impacting what information, if any, was transmitted). And remember, even though a court may certify a class, it can later decertify it.

We are currently defending more than 200 privacy or data security lawsuits. Over 50 of those cases involve Pixel-related issues.

CHAPTER 9

Education

School districts, public and private schools, colleges, and universities face unique issues during the incident response process.

Not just personal information.

Colleges and universities often store large amounts of sensitive research data. Some of that data could be highly classified, triggering an obligation to provide notice to a government entity, such as the Department of Defense. Educational institutions also maintain disciplinary files about both students and employees, which could cause significant embarrassment to the school and the individuals involved if stolen by a threat actor and posted to the dark web, even if legal notification obligations are not triggered given the type of information involved.

Data protected under FERPA is accessed in most ransomware incidents.

Although FERPA recommends (but does not require) schools send notification letters to students whose education records are stolen/subject to unauthorized release, it requires schools to include a notation in student files. Additionally, postsecondary institutions that participate in federal student aid programs must report actual and suspected data breaches to the Department of Education Office of Federal Student Aid (FSA), which generally requests periodic or ongoing reporting of the institution's response to the incident.

Systems are often decentralized, making it difficult to identify data.

Many businesses can readily identify where their most important and sensitive data are stored. Educational institutions—especially large research universities—often have sensitive data stored throughout a decentralized infrastructure. For example, the IT team may have little or no insight regarding the sensitivity or nature of the data that is maintained on the school of engineering's servers. In the immediate aftermath of a ransomware incident, this makes it much more difficult to assess what data was compromised and what devices need to be restored to regain access to the data in the event of encryption.

Leadership structures are not conducive to quick decision-making.

Early in the incident response process, a ransomware victim may need to quickly decide what vendors to engage, whether to pay a ransom, and how to communicate both internally and externally about the incident. Delaying these decisions could result in prolonged service interruptions, data loss, and reputational harm. Consequently, it is vital that educational institutions have an incident response plan in place that clearly defines who is responsible for making specific decisions. Regularly practicing the plan through tabletop exercises is a great way to identify areas that can be updated or improved.

Ransom Payment Prohibitions.

In 2022, North Carolina passed a law prohibiting state agencies and local government entities (including state universities, community colleges, and public school districts) from paying ransoms or even *communicating with* ransomware threat actors. Florida also enacted a law prohibiting state agencies from paying a ransom. New York, Pennsylvania, and other states are considering similar laws.

Educational institutions need to be transparent but avoid over-sharing at the outset of the incident response process.

Most educational institutions take pride in their culture of transparency, which they consider vital to maintaining the trust of students, employees, and the school community at large. During the incident response process, however, it is important that schools be measured in their messaging. Accordingly, it is important that in their ransomware incident response plans, educational institutions articulate a communications strategy that balances their commitment to being open and transparent with the need to avoid messaging pitfalls that could potentially damage their reputation and erode the trust of their community.

Public records laws.

Key decisions in the response process occur "behind closed doors." Upon discovering the incident, for example, educational institutions must determine when to notify the school community and what information to divulge in that communication. Similarly, schools often need to perform cost-benefit assessments regarding whether it is worth paying a ransom to prevent the threat actor from publishing school data on the dark web. Although some communications about these decision points might be protected from disclosure by the attorney-client communications privilege, others (like ransom negotiation transcripts and public relations strategies) may need to be produced in response to a public records request.

Ransomware in Education by the Numbers

	Initial Ransom Demand	Ransom Paid	Days to Acceptable Restoration	Forensic Investigation Cost	Individuals Notified
2021	**$1,588,468** (median: $558,000)	**$196,071** (median: $154,000)	**10.5** (median:8)	**$68,729** (median: $47,520)	**14,168** (median: 1,268)
2022	**$1,791,650** (median: $750,000)	**$281,525** (median: $175,000)	**12** (median: 7)	**$68,695** (median: $53,000)	**9,567** (median: 415)

CHAPTER 10

Tribal Issues

Native American Organizations and Alaska Native Corporations

Data security incidents have unique considerations and implications for tribal entities.

Several tribal entities experienced significant ransomware incidents this past year, and given the overall impression that casinos have access to large amounts of cash, threat actors view tribally owned casinos as favorable victims.

For Native American tribes and Alaska Native Corporations, incident response is not one-size-fits-all. While a tribe itself may be a sovereign nation, most tribes operate complex business ventures, including those in the tourism, mobile gaming, manufacturing, and healthcare spaces, and the general idea that all governmental and commercial activities both on- and off-reservation are protected by sovereign immunity is changing in today's virtual world. For instance, federal courts are now weighing issues related to tribal casinos' operation of online gaming, which may ultimately impact applicability of state and federal privacy regulations.

Data governance and privacy regulations should be top of mind for leadership. Tribes typically hold four classes of data: Commerce (IRS Form W-2 G, contracts); Government (member information, employment); Member Services (health, housing, funding); and Cultural (language records, photo archives). Tribes should invest in determining the value and location of each class of data; it is more than an exercise in data mapping – it is a key element in cyber preparedness. Tribes also should focus on compliance with privacy regulations. Many tribal entities are now working to implement their own privacy laws and assess what risks they might face if a federal privacy law were to be enacted. Tribes can enact laws to direct how they want to protect the data they hold, and compliance with these laws should be incorporated into the incident response plan.

> **“There are over 500 Native American Tribes recognized by the United States. We are seeing an increase in incidents and interest in maturing compliance programs.**

CHAPTER 11

OCR/Healthcare Update

Healthcare privacy and security regulatory activity began slowly in 2022. But by the end of the year, between the *Dobbs* decision, significant regulatory guidance, and the deluge of healthcare privacy class actions, 2022 will have a lasting effect.

Dobbs in the Driver's Seat

The impact of *Dobbs* on the healthcare industry cannot be overstated. While providers, employers, and insurance companies scrambled to reassess the way they provide and record information about women's reproductive healthcare, regulators showed they recognized *Dobbs* as impacting many corners of operations:

Just days after the *Dobbs* decision was published, the OCR reminded covered entities and business associates that the privacy rule *permits*, but does not *require*, them to share PHI when requested by law enforcement officials.

The FTC stated in a July letter that non-HIPAA regulated entities in the health information space "would be hearing" from the FTC if they made false statements about data anonymization, data sharing, or data aggregation to users.

California passed several laws that impact how employers, healthcare providers, and insurance plans respond to law enforcement requests for information about individuals who have sought abortion-related services.

Ransomware Wobbles, Snooping Surges

Ransomware attacks declined significantly through mid-2022, but came roaring back at the end of the year and into the first quarter of 2023. Throughout 2022, however, we saw a significant increase in snooping incidents. Many of these incidents were driven by workforce members (including licensed care providers) looking for and diverting controlled substances, implicating insurance billing, patient safety, and inventory controls. What do ransomware and snooping have in common? Both can be detected early with appropriate auditing of system activity and timely reviews of those audit reports.

Recognized Security Practices – Take Two?

The passage of the HIPAA Safe Harbor amendment in January 2021 (requiring the OCR to consider whether an entity had in place recognized security practices prior to an incident) was warmly welcomed by the healthcare industry. Both newly initiated and years-old investigations asked entities for proof of their recognized security practices. The problem? Entities were not clear on what "recognized security practices" really meant; it turns out, neither was the OCR. In April, the OCR requested public comment on how it should measure security practices, providing the CISO's office a unique opportunity to frame HIPAA Security Rule compliance standards.

State Attorneys General Take an Interest in HIPAA-Regulated Entities

In 2022, we saw a marked increase in the number of state attorneys general interested in healthcare entities' compliance and incident response posture. After providing notification, the attorneys general of Florida, New York, New Jersey, and Texas initiated investigations into HIPAA and state regulatory compliance.

OCR's Right of Access Initiative

BIG PROBLEMS CONTINUE FOR SMALLER ENTITIES

The OCR's Right of Access (ROA) Initiative continued to be a focus in 2022, with 17 such settlements as of the end of December 2022. While many non-ROA settlements have generally involved larger entities — and thus larger monetary assessments — the ROA settlements show a very different trend, exemplified by the entities involved in the 2022 ROA settlements:

Only two of the settlements exceeded $100,000 (one large hospital system, one larger specialty practice), with the remaining 15 settlement values averaging less than $38,000. Our clients have continued to receive ROA requests, signaling that even with OCR's increased focus on reproductive health privacy, ROA continues to be an area of regulatory risk for entities in 2023. In fact, OCR Director Melanie Fontes Rainer said in a December 2022 press release that "[t]he right of patients to access their health information is one of the cornerstones of HIPAA, and one that OCR takes seriously. [OCR] will continue to ensure that healthcare providers and health plans take this right seriously and follow the law".

OCR Enforcement Actions

Outside of ROA settlements, the OCR entered into six enforcement actions and settlements in 2022, many of which underscored that, in the era of network intrusions and ransomware, entities cannot forget the basics:

- Do not publicly respond to online complaints by posting PHI
- Do not use a patient list – even if just demographics – for marketing without an authorization
- Do not dispose of PHI in garbage cans

OCR did not miss two opportunities to remind entities that deficient network activity monitoring, security risk assessments, and risk mitigation plans continue to drive enforcement actions. In fact, the two largest monetary settlements finalized between January 1 and December 31, 2022 ($875,000 in July 2022 and $1.25 million in December 2022) were based largely on alleged deficiencies in those areas.

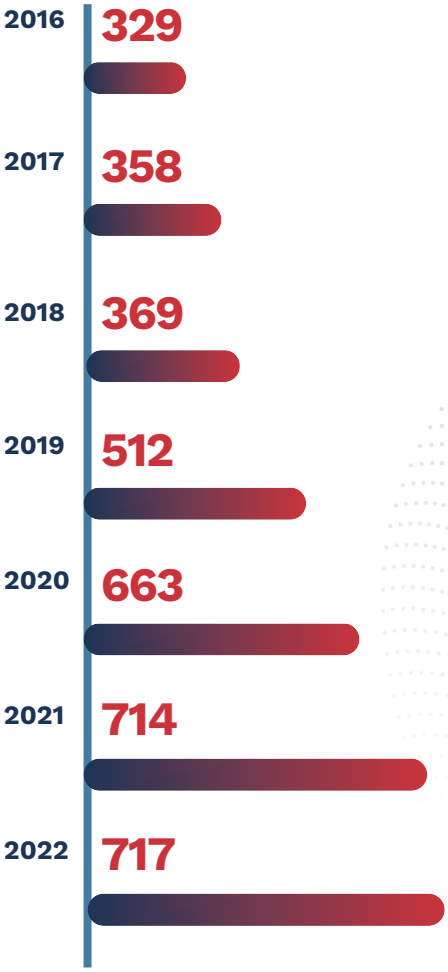
From the first enforcement action in 2008 to the end of 2022

129
(23 in 2022)
Cases settled or imposed a Civil Monetary Penalty

$16M
($1.25M in 2022)
Highest amount paid as part of a resolution agreement

$133.5M
($2.25M in 2022)
Amount collected by OCR through its enforcement actions

HIPAA Breaches of 500+ Individuals Reported to OCR



We helped clients manage more than 15% of the healthcare breaches reported to OCR in 2022.

CHAPTER 12

Securities and Exchange Commission

Increased Regulatory Scrutiny of Cybersecurity Incidents

Historically, the enforcement actions related to security incidents brought by the SEC have been against investment advisers and broker-dealers. However, since 2021, there have been three cases that were resolved with companies agreeing to pay fines related to the adequacy of disclosures regarding material cybersecurity incidents and possibly another enforcement action on the way. According to SolarWinds' October 28, 2022 Form 8-K, the SEC issued a Wells Notice to SolarWinds stating that the SEC had made a preliminary determination to recommend the filing of an enforcement action against SolarWinds alleging violations of certain provisions of the U.S. federal securities laws with respect to its cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures.

The SEC's increased focus on cybersecurity is clear – starting with a January 2022 speech by SEC Chairman Gensler and the announcement that it is adding 20 positions to the Crypto Assets and Cyber Unit. Overall, the SEC investigations and enforcement actions increased in 2022. The SEC filed 462 new enforcement actions, a 6.5% increase from the previous year.

PROPOSED RULES ON CYBERSECURITY DISCLOSURES

In that same January 2022 speech, SEC Chairman Gensler identified the following areas where he anticipated the SEC increasing regulation in connection with cybersecurity:

- Updates to Regulations SCI and S-P, impacting SEC registrants;
- A significant increase in disclosure requirements impacting public companies; and
- Potential new measures to address cybersecurity risks from service providers to include potentially regulating third-party providers.

Following these comments, the SEC released proposed rules intended to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cyber incident reporting by companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. In its press release, the SEC stated the proposed rules are intended to:

- Provide timely notification of material cybersecurity incidents;
- Better inform investors about such companies' risk management, strategy, and governance; and
- Enable investors to assess the possible long- and short-term financial or operational effects of a material cyber incident.

3 out of **118 incidents**

involving companies registered with U.S. or other international stock exchanges resulting in a disclosure of a material event

The proposed rules would add new Item 1.05 to Form 8-K and require disclosure of material cybersecurity incidents within four business days of determining the event is material. In addition, proposed amendments to Regulation S-K, Form 10-K, and 10-Q would require:

- Updated disclosure regarding previously reported material incidents and disclosure of unreported incidents that have become material in the aggregate, and
- Periodic reporting about the following:
  - An issuer's policies and procedures to identify and manage cybersecurity risks;
  - The issuer's board of directors' oversight of cybersecurity risk;
  - Management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures; and
  - The board of directors' cybersecurity expertise, if any.

The SEC's 2018 guidance on cybersecurity disclosures makes it clear that companies must evaluate cybersecurity incidents using both a quantitative and qualitative analysis, as the materiality of a cybersecurity risk depends on its "nature, extent, and potential magnitude, particularly as [it] relate[s] to any compromised information or the business and scope of company operations...and the range of harm that such incidents could cause." While the four-day obligation to file an 8-K disclosing a material cybersecurity event received the most attention from commentors in response to the SEC's proposed rules, it may be the easiest of the new rules to comply with. The new cybersecurity risk management strategy disclosure obligation may be the most challenging of the new requirements because it may be difficult for companies to meaningfully and accurately describe their security strategy without providing too much detail.

Take Action:
Develop Effective Disclosure Protocols.

Define a protocol in the incident response plan

to ensure that incidents that may be material get escalated to the disclosure committee (e.g., for all incidents classified as "high" or "critical," the legal team representative will consider at appropriate intervals whether to review with the disclosure committee).

Ensure that the internal team responsible for SEC filings checks with key incident response team members

before filing the next K or Q to determine if there are any investigations underway or anything that would make forward-looking cybersecurity risks or cybersecurity risk management strategy disclosures inaccurate.

CHAPTER 13

Employer-Sponsored Health Plans

HIPAA Affects More Than Healthcare Providers

Non-healthcare companies may not always understand that certain information related to employee health benefit plans is regulated by HIPAA, and any breach of this data is subject to enforcement and penalties by the Office for Civil Rights (OCR). Just as a hospital must comply with HIPAA's Privacy, Security, and Breach Notification Rules, employer-sponsored health plans are also considered HIPAA "Covered Entities" and must comply with the same regulations, even if the company itself is not a healthcare provider. When a threat actor steals data from directories on a file server used by the HR department and PHI related to the plan is stored there, both state laws and HIPAA's breach notification rule must be considered. These scenarios are fairly common in ransomware incidents, and they greatly increase the complexity of the response effort.

Why Does HIPAA Apply?

So why are manufacturers, technology, hospitality, energy, and financial services companies subject to a "healthcare" law? It's because HIPAA also governs "group health plans," which include **both** fully insured and self-insured employee welfare benefit plans that (1) have 50 or more participants or use a third-party administrator, and (2) provide payment for medical care. The employer, in its role as the plan sponsor or plan administrator, must maintain a HIPAA compliance program and safeguard participant protected health information (PHI).

Most companies use third-party administrators (e.g., United Healthcare, Blue Cross) to administer claims on behalf of the health plan. Enrollment and claims information is subject to HIPAA. The third-party administrator is the plan's Business Associate, and the plan is the covered entity (bearing liability for a breach).

Regulators Are Actively Investigating Employer-Sponsored Plans

The OCR has likely seen an increase in breach notifications from employer plans, and post-incident investigations now are being opened on a routine basis (some with fewer than 500 individuals involved). We are also seeing follow-on investigations from the Department of Labor with a focus on the plan's overall cybersecurity posture.

> **Employer-sponsored health plans are considered HIPAA 'Covered Entities' and must comply with the same regulations, even if the company itself is not a healthcare provider.**

Take Action: Conduct a Risk Assessment.

Prioritize a review of all data held by human resources and other internal departments with access to plan-related information to identify what is covered by HIPAA and determine whether a sufficient compliance program is in place. All companies should:

Assess Their Benefit and Wellness Programs

Identify benefit offerings subject to HIPAA, as the regulations cover more than just "health insurance." Covered plans may include health, dental, vision, employee assistance programs, health reimbursement arrangements, wellness programs, and health spending accounts.

Track Plan Information

Identify where, why, and to what extent plan PHI is created, received, maintained, or transmitted by the plans and Business Associates. The discussion should involve IT, finance, HR, legal, and other departments that may handle PHI as part of their job functions. Look for files with enrollment information, high-spend reports, and claims information. Apply a retention program and get rid of files no longer needed.

Implement a Compliance Program

The program should include appropriate policies and procedures based on the type of plan, HIPAA-specific training, and an annual HIPAA security risk analysis and risk management plan. Companies should also review their plan documents to ensure they include the HIPAA-required components and certification.

> **"We are seeing follow-on investigations from the Department of Labor with a focus on the employer plan's overall cybersecurity posture.**

CHAPTER 14

Global Privacy

International Data Protection

May 25, 2023 will be the fifth anniversary of the effective date of the European Union's General Data Protection Regulation (GDPR), a law that led the way (and has frequently set the standard) for scores of data protection laws that have since been implemented around the world. For the past five years, many global companies have been operating in a perpetually reactive privacy compliance posture, with new laws coming online faster than full compliance programs can be built and operationalized. As a result, privacy governance efforts often target specific obligations without developing a holistic approach for meeting all (or even most) requirements of the law. As the data protection legal landscape continues to evolve, global companies need to assess and improve the maturity of their privacy compliance programs as part of ongoing risk management efforts.

ENFORCEMENT AGENDA

Greater Coordination Among European Regulators.

Although historically, data protection authorities (DPAs) have largely focused on policing serious infringements brought to their attention through individual complaints, personal data breach notices, or media exposés, we are starting to see a shift in regulatory agendas toward the proactive use of investigative and corrective powers. Throughout 2022, the effectiveness of the European Member State DPAs and their ability to enforce the GDPR were debated in the European Parliament and in the media. Newer laws, such as the European Union's Digital Services Act and Digital Markets Act, rely more heavily on a centralized regulatory body, and many have proposed that the GDPR might benefit from similar reforms. In response, Member State DPAs are moving toward a more coherent and coordinated GDPR enforcement strategy, including cooperation among the regulators and simplification of their enforcement action processes. As part of this effort, the European Data Protection Board established criteria for determining investigation and enforcement priorities, such as the recurring nature of an alleged violation, whether it intersects with other legal obligations (for example, consumer protection), and the level of risk to individuals.

Enforcement Priorities.

Many regulators annually publish their enforcement strategies for the upcoming year or annual reports highlighting their enforcement activities. In Europe, DPAs are clearly prioritizing inspections and sanctions. As a general matter, DPAs expect to see more workforce awareness and internal training to address privacy and data security compliance in an anticipatory manner. The European Data Protection Board has indicated that it will be focusing an upcoming coordinated action on the designation and position of data protection officers – whether they have been properly appointed and are being appropriately deployed within companies.

MEMBER STATE DPA ENFORCEMENT EMPHASIS ON:

- Personal data transfers, especially in the context of cloud-based technologies;
- The privacy of children and other vulnerable populations, including age-appropriate design, restrictions on profiling and data sharing, and use of CCTV in care spaces;
- Advertising technologies, including dark patterns, online marketing, and data brokers;
- New and emerging technologies, such as artificial intelligence, digital identities, blockchain, smart cities, and biometric information; and
- Compliance documentation, such as data protection impact assessments and records of processing activities.

KEY PRIORITIES: ADVERTISING TECHNOLOGIES, EMERGING TECHNOLOGIES, AND COMPLIANCE DOCUMENTATION

Advertising Technologies.

Advertising technologies continue to be a priority for many regulators. Regulators in Brazil, California, China, and South Korea have all recently called out data use by online advertising technologies and mobile apps as an area in need of regulatory attention. AdTech has been the subject of a great deal of guidance published by DPAs. Such guidance is often dismissed as non-binding, but companies should take note that these publications are key to understanding regulatory expectations. Moreover, this guidance is often enforceable. Recent guidance has closely paralleled both the enforcement actions we have seen from regulators and their stated enforcement priorities. Accordingly, we expect regulators to focus on the following areas related to advertising technologies in 2023:

- Protecting individual rights when using digital products and services;
- Online tracking and transparency, in particular phasing out third-party cookies and providing functional privacy choices to users;
- Processing personal data from website visitors and app users and providing meaningful choices to people regarding that processing;
- Preventing dark patterns and other deceptive designs;
- Further alignment of regulatory positions on the use of cookies;
- Investigating data brokers and resellers; and
- Preventing unwanted text messages, telemarketing, and other marketing communications.

New and Emerging Technologies.

New and emerging technologies remain a focus for regulators as well, especially technologies that involve novel uses of personal data. Regulators have continued to highlight the close relationship between personal data and digitalization. For many companies, the successful implementation of newer, data-driven technologies will demand a mature privacy compliance program to build on. Several regulators, including DPAs in France, the Netherlands, Norway, and Spain, have or will be creating special units focused on AI oversight and enforcement. With respect to other areas requiring subject-matter expertise, the European DPAs will be able to call on a support pool of experts for assistance with investigations. Regulatory priorities related to newer and emerging technologies for 2023 include:

- Predictive algorithms and AI, particularly in automated business applications and processes;
- The collection of personal data through smartphones and apps;
- Emerging types of data collection, such as emotion recognition;
- Biometric technologies;
- New uses of health data; and
- Anonymization and pseudonymization standards.

> **“The successful implementation of newer, data-driven technologies demands a mature privacy compliance program as a foundation upon which to build.**

Internal Compliance.

Finally, a number of regulators have stated their intention to investigate internal compliance at both public- and private-sector companies. Regulators tend to do this by issuing questionnaires, requesting internal documentation, and/or initiating formal or informal investigations. We have seen growth in this type of action following personal data breach notifications. We expect regulators to use these tactics more frequently as part of their proactive compliance checks.

ENFORCEMENT PRIORITIES INCLUDE:

- **Questionnaires and Inspections Related to Employee Data**
- **Data Retention Practices**
- **Reviewing Unreported Personal Data Breaches**
- **Compliance Documentation**

Essentially, if documentation is required by law, companies should expect regulators may ask to review it. Among other things, they may ask to examine internal policies and procedures as well as any required compliance materials, such as data protection impact assessments, transfer impact assessments, records of processing activities, and personal data breach records. These types of internal documents are not often the top priority for many companies, but they can become critical to demonstrating compliance or justifying actions that may have created or mitigated privacy risks.

Looking Ahead

Regulators outside of Europe also have initiated similar proactive strategies. South Korea's Communications Commission, for example, created a cell phone personal data breach prevention program in late 2022 aimed at finding ways to minimize such breaches in the future. South Korea's Personal Information Protection Commission has recently revised its guidance on technical and organizational safeguards as well as its guidelines on using employment and healthcare data, indicating potential areas of upcoming regulatory focus. Brazil's DPA highlighted several areas in its agenda for 2023-2024, including international personal data transfers, data protection impact assessments, data protection officers, AI, and developing minimum technical security standards. China continues rolling out regulations related to its recent privacy and cybersecurity laws, including releasing a standardized contract for cross-border personal information transfers. In the upcoming year, we expect to see corresponding scrutiny and enforcement in China.

As new privacy and data protection laws continue to emerge – watch out for pending legal reforms in Australia and Canada, a revised law in Switzerland, and a possible new law in India in 2023 – companies should be taking stock of their privacy compliance programs. Decide what is working and fix what is not. Think about how to streamline your compliance program for improved functionality, considering both applicable data protection laws and your overall risk mitigation strategy. Reacting to changes in the legal landscape will be much less burdensome if you already have a functional, mature privacy compliance program that simply requires modification to meet new challenges.

CHAPTER 15

U.S. Employee Privacy Roundup

Employee and Applicant Data Comes into Scope Under the California Consumer Privacy Act (CCPA)

January 1, 2023 marked the expiration of an exemption to the CCPA that excluded personal information about employees and job applicants from most of CCPA's compliance requirements. As a result, employers must now provide all CCPA rights to their California workers, including prospective, current, and former employees, as well as temporary workers. Employers who have not yet mapped their data, built processes for handling employee and applicant privacy rights requests, and updated privacy notices for these populations should do so as soon as possible. With enforcement authority now vested in both the California Attorney General and the California Privacy Protection Agency (CPPA), the risk of non-compliance is heightened as well. Enforcement of these expanded requirements under the amended CCPA will begin on July 1, 2023. Fortunately for employers, California is currently the only state whose comprehensive privacy law applies to employee and applicant personal data. The comprehensive privacy laws taking effect in 2023 in Virginia, Colorado, Connecticut, and Utah all exempt employee and applicant data from their scope.

New York Employee Monitoring and Automated Decision-Making

Joining Connecticut and Delaware, New York State passed an amendment to its Civil Rights Law, effective May 7, 2022, requiring private-sector employers that monitor their employees' use of telephones, emails, and the internet to provide prior written notice of such monitoring and obtain acknowledgment of receipt of the notice. The law applies to employers with a place of business in New York but exempts data monitored solely for the purpose of system maintenance or security. Given its broad scope, New York employers are likely subject to this law and should assess its applicability to their monitoring activities, prepare updated disclosures, and obtain acknowledgments as needed. Meanwhile, in April 2023, New York City began enforcing Local Law 144, which took effect on January 1, 2023. Local Law 144 regulates the use of automated employment decision tools (AEDTs) and requires employers to provide notices and undertake audits to identify potential bias associated with the use of AEDTs.

BIPA Class Action Reaches Jury Verdict Favoring Employee Class

In October 2022, the first jury trial on a case alleging violations of the Illinois Biometric Information Privacy Act reached a $228 million verdict in favor of a class of employees. The jury found the employer violated BIPA by scanning and retaining employees' fingerprints at its locations without obtaining written informed consent and without publishing a data retention or destruction schedule. At trial, the employer unsuccessfully argued that it could not be held liable because the fingerprints were scanned by a third-party vendor, which underscores the need for employers to understand their responsibility for the consent and destruction requirements under BIPA. The case also serves as a reminder of the ongoing importance of BIPA compliance even as the law approaches its 15th anniversary.

CHAPTER 16

FTC Update

Aggressive FTC Rulemaking Agenda

For the first time in decades, the Federal Trade Commission (FTC) has initiated multiple new rulemakings covering a wide range of industries and issues. These rulemakings (which, if completed, would allow the agency to seek civil penalties for violations) will continue into 2023 and beyond. The rulemakings include:

Commercial Surveillance

A broad rulemaking focused on a wide range of privacy and data collection issues with an emphasis on the use of data for advertising purposes.

Unfair or Deceptive Fees *(Junk Fees)*

A rulemaking exploring whether and how to ban a wide range of fees that are charged to consumers in various contexts that "have little or no added value to the consumer, including goods or services that consumers would reasonably assume to be included within the overall advertised price."

Reviews and Endorsements

A rulemaking focused on deceptive or unfair review and endorsement practices, with an emphasis on potential unlawful practices regarding online reviews.

FTC Emphasis on Online Dark Patterns

For the past year, the FTC has focused extensively on dark patterns, which are generally described as online interfaces that manipulate consumers into making decisions they would not otherwise make or that lead to consumers sharing more data than they intended. The contours of what constitutes a dark pattern that violates the law are not particularly well-defined, and a September 2022 FTC report on the topic did not provide real clarity. Two recent FTC law enforcement actions do shed some light on what practices the FTC finds deceptive or unfair. In one case, the FTC settled for $100 million and alleged that a company made it easy for consumers to sign up for services but difficult to cancel through the use of dark patterns. In a $3 million settlement in a different matter, the agency alleged that, through dark patterns, a company falsely represented to consumers that they had been preapproved for certain credit offerings. The focus on dark patterns will continue in 2023.

FTC Focus on Health and Geo Data

For decades the FTC has focused on the privacy of health data and has also focused a good deal on the privacy of location data. As noted previously, the FTC has focused even more on these issues since the *Dobbs* decision and will continue to do so. Shortly after the decision was announced, the FTC's then-acting associate director of the Division of Privacy & Identity Protection announced in a blog post that websites sharing health, location, and highly sensitive data without adequate disclosures to consumers would "hear from" the FTC. A recent case, which for the first time alleged a violation of the agency's Health Breach Notification Rule, also claimed that the company unlawfully shared health data with third-party advertisers. And in a case currently in litigation, the FTC alleged that the company unlawfully shared consumer geo data with third parties, which could be used to trace individuals to sensitive locations.

CHAPTER 17

Information Governance – Record Retention Risks Closer to "Home"

The GDPR incorporates something colloquially known as the "Storage Limitation Principle" in Article 5.1.(e), which states personal data should only be retained long enough for the purpose for which it was collected. The GDPR's Recital 39 further requires that data storage be "limited to a strict minimum" and notes that "time limits should be established by the controller for erasure or for a periodic review."

Domestically, this is mirrored somewhat in the text of the CCPA (as amended and expanded by the California Privacy Rights Act (CPRA)), which provides, under § 1798.100, that subject organizations must disclose how long the organization "intends to retain each category of personal information, including sensitive personal information, or if that is not possible, the criteria used to determine that period." The current CPRA/CCPA regulations also consider record retention limitations, beginning with § 7001(o), where "Information Practices" includes the retention of personal information, and § 7002(a) and § 7002(d) both address how that retention "shall be reasonably necessary and proportionate."

Why does it matter that the CPRA/CCPA seems to adopt GDPR sensibilities? There is a growing expectation that the CPPA, the enforcement body for the CPRA/CCPA, will evaluate these requirements according to how the GDPR's similar requirements were enforced. Recent 2022 European fines and enforcement actions tell a compelling tale and should warn U.S. organizations accordingly. Among those actions, the following related to information governance and retention:

- The Hungarian Supervisory Authority imposed a fine of approximately €248,000 on internet and broadcasting service providers for the creation and lack of immediate deletion of a database test.
- The French CNIL imposed a €600,000 fine against an electric utility in France for, among other issues, retention compliance problems.
- The French CNIL imposed an €800,000 fine against a French VOIP company for retention compliance problems.
- The Italian Supervisory Authority imposed a €2 million fine on a social media network in part for retention compliance issues.
- The UK Supervisory Authority (ICO) imposed a fine of more than £7.5 million on a facial recognition company for, among other issues, lack of clear data retention policy documentation.
- The French CNIL fined the Trade and Companies Register €250,000 for issues relating in part to retention of data longer than applicable retention periods.
- The French CNIL fined a short-term vehicle rental company €175,000 in part for a lack of implemented proportionate data retention periods.

Two lessons are clear:

01. France is particularly concerned with retention period application.

02. Enforcement in this area is alive and well.

CHAPTER 18

National Advertising Division Trends

Fast-Track SWIFT Takes Off

2022 marks the second full year of Fast-Track SWIFT and Complex Track options for Challengers in addition to the traditional Standard Track. Use of the SWIFT program continues to grow, representing 12% of the cases the National Advertising Division (NAD) decided in 2022. In 2023, we can expect to see some changes in the SWIFT procedures reflecting the NAD's experience handling these cases, which are decided in less than a month, including expanding SWIFT jurisdiction in appropriate cases to implied claim challenges. The Complex Track is slower to take off with only a few cases opting into this process, which is decided by a collaborative panel of NAD staff lawyers. The Standard Track continues to be the primary choice for Challengers, making up 68% of the cases NAD decided in 2022.

FTC Referrals Decline

In the last two years, the number of FTC referrals is down considerably, with only two referrals in 2022 and four in 2021 (whereas prior years generally saw about 10 referrals). Appeals also seem to be trending downward. In 2022, there was around a 40% drop in appeal filings from 2021.

CASES BY INDUSTRY

NAD's docket is consistently heavy with telecommunications challenges, and this year was particularly active, with almost 30% of the docket being telecom cases. Over 40% of the remaining cases fell into four categories.

27%
Telecom

13%
Food/Beverage

12%
Drugs/Health

9%
Dietary Supplements

8%
Household Products

Trends in Case Filings

2022 marked the first year in recent memory that NAD looked at cases involving privacy and data security advertising claims. Perhaps reflecting concerns with the state of the economy, 17% of the cases included a challenge to pricing or value messages. While always a staple at NAD, a surprising 22% of the cases involved superiority claims and another 21% involved health-related claims. NAD focused a good amount of time in its monitoring program looking at environmental and sustainability claims, with such cases representing about 11% of the docket.

CHAPTER 19

State Privacy and Data Collection Legislative Update

In 2022, companies prepared for three new privacy rights to take effect January 1, 2023, under the amended CCPA.

THE RIGHT TO OPT OUT OF SHARING

The amended CCPA includes a new defined term — "sharing" — and provides consumers the right to opt out of sharing. The term "sharing" was added to address arguments that behavioral advertising is not a sale. Sharing means "disclosing… a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration…." "Cross-context behavioral advertising" means targeting of advertising to a consumer based on the consumer's personal information obtained from their activity across businesses, different websites, applications, or services, other than the business, with which the consumer intentionally interacts. There are two key components to the definition of sharing: (1) the explicit language that sharing, unlike selling, does not require any consideration, and (2) the purpose for the transfer must be cross-context behavioral advertising.

Businesses that engage in sharing are required to provide a link on their websites titled, "Do Not Sell or Share my Personal Information," which must immediately effectuate the consumer's right to opt out of sales/sharing or direct them to where they can learn more about the right and make that choice. Businesses must provide two or more designated ways for consumers to submit a request to opt out of the sales/sharing of their personal information to third parties for cross-context behavioral advertising. Usually, this is effectuated through a cookie preference center and/or a request form that consumers can access by clicking on the "Do Not Sell or Share my Personal Information" link but must also be recognized via an opt-out preference signal. Lastly, access and transparency obligations apply to shared personal information as if it was sold personal information.

THE RIGHT TO CORRECTION

The amended CCPA provides a new right for consumers to request that a business correct personal information that it maintains about the consumer. The right is similar to what exists under the GDPR and also exists under the new 2023 privacy laws in Virginia, Colorado, Connecticut, and Utah. When a business receives a request to correct, they need to consider the nature of the personal information and the purposes for processing it. Businesses must disclose to consumers that this right exists and must use commercially reasonable efforts to fulfill verifiable requests.

THE RIGHT TO LIMIT USE AND DISCLOSURE OF SENSITIVE PERSONAL INFORMATION

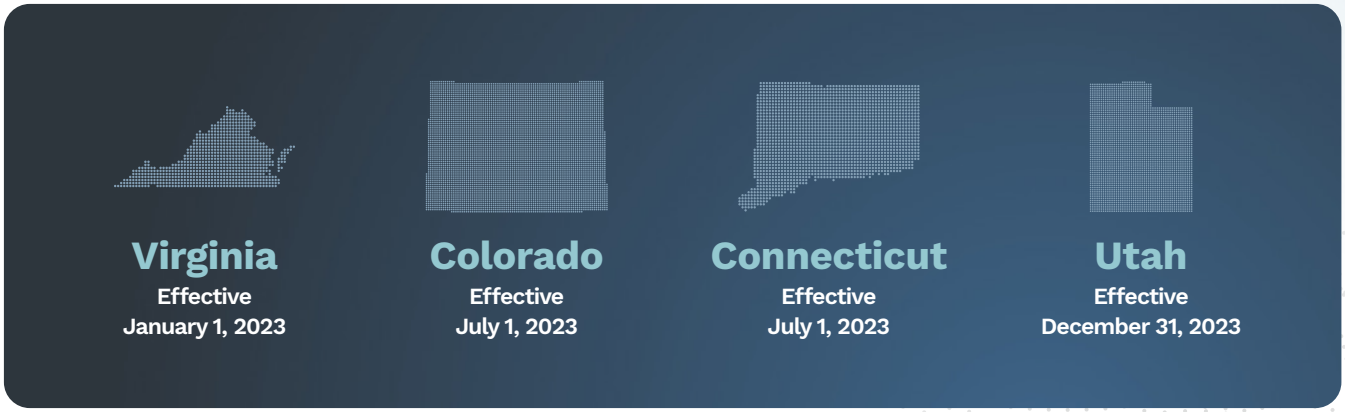
The amended CCPA provides a new defined term of "sensitive personal information" and imposes new obligations on businesses processing sensitive personal information, which now includes:

- Social Security, driver's license, state identification card, or passport numbers;
- Account log-in, financial account, debit card, or credit card numbers in combination with any required security or access code, password, or credentials allowing access to an account;
- Precise geolocation (radius ≤ 1,850 ft.);
- Racial or ethnic origin, religious or philosophical beliefs, or union membership;
- The contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication;
- Genetic data;
- Biometric information processed for the purpose of uniquely identifying a consumer;
- Personal information collected and analyzed concerning a consumer's health; and
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

The amended CCPA provides consumers the right to request that a business limit the use and disclosure of their sensitive personal information. Specifically, a consumer can direct a business to use sensitive personal information only for purposes necessary to perform the service or provide the goods requested or as set forth in 1798.140(e)(2)(4)(5), and (8). Businesses that process sensitive personal information for purposes that are not necessary to perform the service or provide the goods requested or as set forth in 1798.140(e)(2)(4)(5), and (8) will be required to provide a link on their homepage(s) titled, "Limit the Use of My Sensitive Personal Information."

Four More State Privacy Laws Take Effect in 2023

In 2022, companies began preparing for four new comprehensive privacy laws in Virginia (effective January 1, 2023), Colorado (effective July 1, 2023), Connecticut (effective July 1, 2023), and Utah (effective December 31, 2023). Inspired primarily by the CCPA and the GDPR, these laws extend data privacy rights to consumers in their respective states, including the right to access, right to delete, right to correct, and right to opt out of targeted advertising. Although all four laws – and the CCPA – appear to share common goals of consumer protection, greater transparency, increased control over personal data and limiting targeted advertising, there are significant differences among each of these laws related to the right to opt out of profiling, recognition of automated browser signals, and Data Protection Impact Assessments (DPIAs).



California's Age-Appropriate Design Code Act

On September 15, 2022, Gov. Gavin Newsom signed into law the California Age-Appropriate Design Code Act (AADC), which will take effect on July 1, 2024. Inspired by (though not identical to) a similar law in the United Kingdom, the AADC seeks to promote online safety and privacy for children under 18 years of age. Covered businesses will be required to complete a DPIA and may need to make changes to their online services and products.

The AADC applies to any business that meets the revenue or data-collection thresholds created by the CCPA and that "provides an online service, product[ ] or feature likely to be accessed by children." The act covers not only services directed to children but also general-audience websites, apps, and online services that are routinely accessed by a significant number of children, have a "significant amount" of child users, are "substantially similar" to services known to be accessed by children, advertise to children, or have design elements known to be of interest to children.

Although the AADC does not include a private right of action, civil penalties are stiff – up to $2,500 per affected child for each negligent violation and up to $7,500 per affected child for each intentional violation. Although there is a 90-day right-to-cure provision, the Attorney General may demand a list of all DPIAs completed by a business within three business days and copies of all DPIAs within five business days.

The AADC is currently subject to a legal challenge by a consortium of online businesses alleging that it improperly restrains free speech, among other issues.

CHAPTER 20

Digital Assets: NFTs, Crypto, Blockchain

Incidents Involving Blockchain and Digital Assets

By all accounts, 2022 registered as one of the most turbulent years in crypto history. Several large centralized cryptoasset firms imploded as traditional markets floundered, unleashing a contagion[1] that reverberated around the world. Meanwhile, reports indicate that the total value stolen in cryptocurrency hacks achieved an all-time high of $3.8 billion. Crypto-related scams continued to evolve in sophistication, and the volume of illicit cryptocurrency transactions grew to a record $20.6 billion, 43% of which was tied to sanctioned persons and entities. In response to such threat actors, the U.S. government fired a warning shot in the direction of decentralized protocols by sanctioning a well-known decentralized cryptocurrency mixer, a precedential action that resulted in the first instance of software being sanctioned.

DeFi Protocol and Bridge Hacks

Decentralized finance (commonly referred to as "DeFi") protocols, which operate autonomously through code that facilitates various types of digital asset transactions without assistance from third-party banks or other intermediaries, offer novel solutions to keyman, honey pot, and other risks inherent to centralized financial institutions. However, DeFi's reliance on code to mediate transactions and the dearth of oversight over DeFi markets render the ecosystem vulnerable to code exploits and other malicious activity, often with little legal recourse or opportunity to remediate resulting harms. With DeFi hacks representing approximately 82% of all crypto hacks in 2022, the risks these platforms represent are a growing concern.

CROSS-CHAIN BRIDGE HACKS

Crypto "cross-chain bridges" facilitate the creation of liquid markets by allowing users to deposit one type of cryptoasset as collateral to obtain a synthetic representation of that asset on a different blockchain quickly and efficiently for easy trading in DeFi ecosystems. As such, DeFi markets rely on cross-chain bridges to provide critical infrastructure that underpins all market activity. However, by design, cross-chain bridges often store collateralized assets in a central repository, making them lucrative targets for sophisticated hackers seeking quick paydays. Additionally, their reliance on code to facilitate asset transfers, rather than third-party intermediaries, render them vulnerable to hackers. Such vulnerabilities explain why a reported 64% of DeFi hacks were attributable to hacks or exploits of cross-chain bridges in 2022.

One of the biggest bridge hacks in 2022 manifested after a project published a code update that exposed a critical vulnerability that had not yet been remediated. The vulnerability allowed a hacker to mint approximately $325 million worth of derivative cryptoassets on a particular blockchain without depositing the requisite collateral. Such exploits, which can quickly deplete large amounts of liquidity from a given bridge, may leave founders and project backers scrambling to replenish stolen assets to prevent potential cascading effects, such as severe downward market volatility, eradication of traders' positions, and other contagion-like effects. Another major bridge hack in 2022 resulted in the theft of approximately $625 million worth of cryptoassets from an Ethereum sidechain bridge. Details of the event unfolded over the course of a year, exposing a complex criminal scheme the U.S. government eventually tied to a North Korean-sponsored threat group. The hack, a result of a sophisticated "spear-phishing" scheme that targeted developers with access to core infrastructure associated with the DeFi bridge, is demonstrative of several serious risks DeFi platforms pose to both consumers and national security.

[1] *"Contagion" as used here refers to a financial crisis that creates a ripple effect, spreading the crisis to other firms, markets, or regions.*

The scheme involved the hackers presenting a seemingly legitimate and lucrative employment offer to the developer who downloaded materials about the "offer." The content contained a trojan horse that granted hackers access to the developer's device, which contained credentials the hackers stole and used to gain unauthorized access to a crypto wallet holding significant value.

Hacks have exposed various flaws in the DeFi ecosystem. One key vulnerability appears to be when purportedly "decentralized" projects use substandard protocols that result in a centralized attack vector. As demonstrated above, this can expose DeFi projects to the same types of risks faced by centralized entities.

DEFI "FLASH LOAN" HACKS

DeFi "flash loans" are uncollateralized digital asset lending programs deployed on a blockchain. They provide instant liquidity to borrowers and execute instant trades on their behalf. If the borrowed digital assets are not repaid, or if the executed trade is unprofitable, the underlying code of the flash loan considers the terms of the loan unsatisfied, reverses the transaction and returns the borrowed digital assets to the lender. While DeFi flash loans present a theoretically low risk of financial loss to lenders and borrowers who use them as intended, their reliance on code and underlying network governance mechanisms may present significant hacking risks.

One such risk relates to coding or design flaws in the voting mechanisms used by DeFi network participants to make collective decisions concerning network upgrades or treasury allocations. In one example, the exploitation of a majority governance system implemented by one DeFi protocol led to the loss of $182 million of the protocol's native governance token and left the rightful owners of those tokens holding the bag. The vulnerability was exploited through use of a flash loan, which allowed the hacker to borrow nearly $1 billion in digital assets and exchange them for 67% of the DeFi protocol's voting stake in the project. Now having acquired more than the two-third's control required to unilaterally approve code executions, the hacker was able to access the project's wallet and steal the funds. The theft left the project devastated for several months.

PHISHING AND ROMANCE SCAMS

While reports indicate that crypto scam revenue fell nearly 46% in 2022, phishing scams continued to make headlines. For example, in May 2022, scammers stole approximately $4.3 million of cryptoassets by using social engineering tactics to lure victims to a fraudulent website designed to trick them into granting access to their crypto wallets. Romance scams also continued in 2022. In a crypto "romance scam," the attacker establishes a close relationship with their victim, sometimes over the course of months. Once the victim's trust is gained, the attacker manipulates the victim into sending them large sums of cryptoassets.

CRYPTO-JACKING

Crypto-jacking refers to the installation of cryptocurrency mining malware on a user's device without the user's consent or knowledge. The unauthorized software is typically installed after the user unwittingly visits a malicious website or falls victim to a phishing scheme. It is programmed to mine cryptocurrency (a resource-intensive activity) for the benefit of a threat actor over a long period of time without raising the suspicion of the user. According to reports, in 2022, crypto-jacking incidents increased by 30%, with the retail sector suffering from a 63% increase and the financial sector witnessing a 269% increase.

MONEY LAUNDERING AND SANCTIONS EVASION

Digital assets continue to be used by threat actors in money laundering and sanctions evasion schemes. According to one report, in 2022, a single infrastructure protocol alone facilitated the laundering of more than $540 million in cryptoassets derived from theft, fraud, ransomware, and other illicit activities during a span of approximately one-and-a-half years. In another notable event, on Aug. 8, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned a well-known decentralized digital asset mixing service, alleging it was used to launder more than $7 billion worth of cryptoassets since its 2019 inception. The action marked the first instance of OFAC asserting that decentralized software (i.e., code deployed on and accessed through immutable public blockchains) can be sanctioned.

CHAPTER 21

Transactional Data Privacy and Security Update:

Drowning in Data Processing Addendums

Privacy and commercial transactions attorneys have spent the last year inundated with addendums. It has become common for businesses to address privacy requirements by slapping a data processing (or "privacy" or "security") addendum on an otherwise form contract.

The practice is especially evident in digital services where third parties are collecting, hosting, or otherwise processing data on behalf of a business. The continued concern for data breaches combined with the evolving coverage of state and federal privacy laws have turned the trickle of DPAs from the past few years into a tsunami.

On the one hand, few would argue that the increased attention on breaches, privacy, and data security in contracts is a bad thing overall; on the other hand, however, the lack of uniformity, potential conflict with other contract terms, inconsistencies in the laws, incorporation by reference, and year-over-year updating have caused confusion and headaches for transactional privacy lawyers and their corporate counterparts. Of course, some businesses still include applicable and necessary privacy and security terms in their master agreement rather than in a DPA, but the speed at which privacy law and security technology are evolving has established the data privacy/security addendum as the preferred method for negotiating privacy and security terms in contracts.

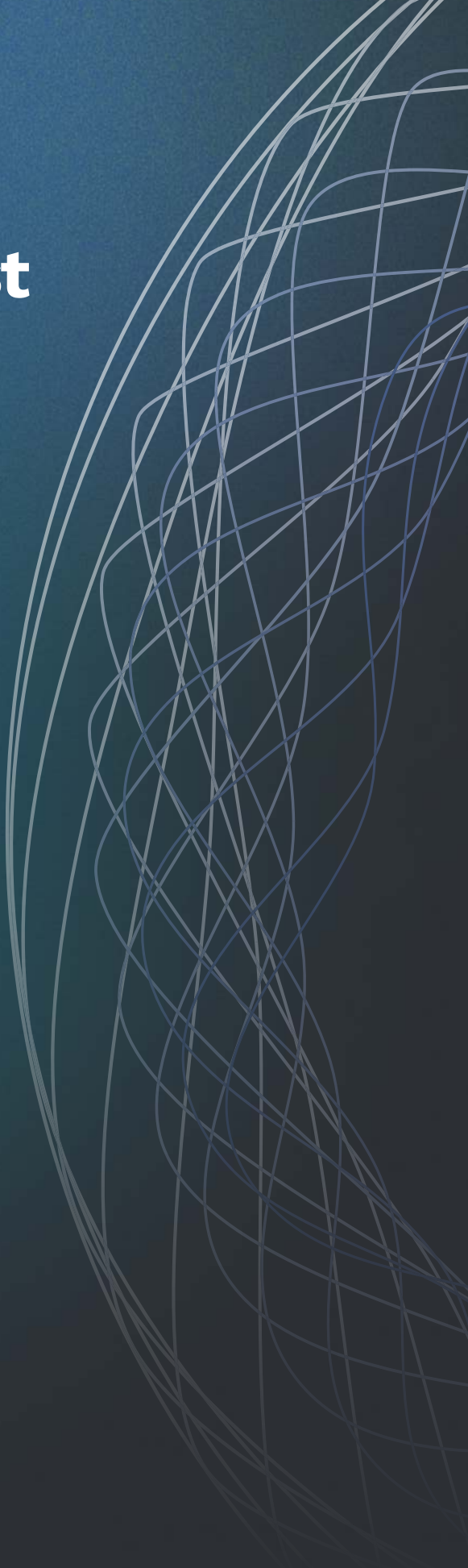
DPAs are often considered through the lens of privacy statutes and regulations, but these documents also often deal with important topics like data security measures and rights and obligations in the event of a data security incident. When a data security incident occurs, a business not only needs to determine what data and third parties may be involved, but also the applicable notification terms in the contracts (including DPAs) with any potentially involved third parties. The incident notification terms in the DPA may differ from those under applicable laws.

For international businesses and businesses with a presence in the EU, variations of DPAs have been fairly common since GDPR came into effect. For U.S.-centric businesses, the practice didn't become widespread outside of a few specific industries (e.g., HIPAA requirements for healthcare entities and state and federal requirements for certain financial services) until CCPA became law. CCPA (as amended by CPRA) made proper privacy and security contract terms imperative for businesses sharing personal information with vendors. Without the proper privacy contract language in place, sharing data with a vendor could be considered a "sale" of personal information, giving rise to a number of additional obligations under CCPA. Companies that do not otherwise sell personal information are incentivized to ensure the proper contractual language is in place with all vendors to avoid inadvertently doing so. Under CPRA, even when a company is selling personal information, the contract must include specific privacy and security terms. In light of this, you would be hard-pressed these days to find a contract between sophisticated parties for services involving personal or sensitive information without some additional data privacy or security terms.

The matter is further complicated, though, because the contractual requirements under data privacy laws have evolved over the last couple of years. While the basic requirements for contracting between controllers and processors under GDPR haven't materially changed since the law went into effect, the transfer mechanisms have changed, and that has had a significant impact on DPAs for companies subject to GDPR. Similarly, in the U.S., the service provider contracting requirements required under CCPA were modified by CPRA and the draft implementing regulations that go into effect this year. Additionally, other comprehensive state privacy laws (e.g., Virginia, Colorado, etc.) have requirements (and definitions) that are significantly different from California's. These statutory requirements are all fairly specific regarding the language that should be used in these contracts. For example, recent updates in CPRA require specific auditing rights, review, and monitoring of the DPAs and privacy compliance. Thus, businesses that signed a CCPA-compliant DPA prior to CPRA may need to update those terms. It also means these addendums require continuous monitoring and testing – these are no longer sign-and-forget contracts.

DPA review and approval can be a challenging process for privacy and transactional attorneys because DPAs come in different shapes and sizes. Some DPAs only contain the required privacy language – others also include substantial security terms and commercial terms. There is no one-size-fits-all DPA, and companies need to establish a process for evaluating DPAs and a benchmark for when DPAs are acceptable and when they should be negotiated.

DPA Review and Negotiation Checklist



- **Determine the roles of the parties**
  Which party is the business/controller and which party is the service provider/processor? Is the business/controller selling personal data or sharing it for a business purpose?
- **Determine which party's DPA will apply**
- **Determine the applicable laws**
  EU/UK, U.S., both, other?
- **Determine the scope of the DPA**
  Privacy, security, both? Identify and note any applicable incident notification terms.
- **Does the DPA only cover required privacy terms**
  or does it also include negotiatble terms like indemnification?
- **Confirm that the DPA covers all requirements for applicable laws**
  For a California DPA, this would include, among other things, the requirements in Section 7051 or 7052 of the regulations.
- **Review the order of precedence**
  for commercial and legal terms also covered in the main agreement.
- **Review for material changes**
  to terms also covered in the main agreement.

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

Joseph L. Bruemmer
Cincinnati
T +1.513.929.3410
jbruemmer@bakerlaw.com

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

Sara M. Goldstein
Philadelphia
T +1.215.564.1572
sgoldstein@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

Linda A. Goldstein
New York
T +1.212.589.4206
lgoldstein@bakerlaw.com

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
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

Jeewon Kim Serrato
San Francisco
T +1.415.659.2620
jserrato@bakerlaw.com

BakerHostetler
bakerlaw.com