
Digital Assets and Data Management – Resilience and Perseverance



Key Findings



MFA. It is expected, and the question now is whether “push notification” is sufficient.



Ransomware groups are moving quickly. Can you stop them before they detonate?



Litigation on the rise. Smaller incidents are yielding class action lawsuits.



Hi, it's ransomware calling. Threat actors are contacting your employees and customers directly if you do not engage.



You have EDR? That's great. Now who's monitoring it and how is it configured?



Oh, you don't have EDR? That's worth a second look.



Immutable backups. You have a better chance of recovering your data if it can't be changed or deleted.



Ransom payment amounts drop. Companies have improved their ability to restore from backups. Payments for a decryptor are more expensive than only paying to prevent disclosure.



Ransomware groups remain reliable criminals.

Threat actors provided decryptors and didn't default on promises to not publish stolen data 97% of the time.



Zero trust gaining traction. More organizations are starting down the path to implementation. Are you?



Double or triple extortion.

Ransomware threat actor groups want your money and are trying more ways to get it (encryption, exfiltration, and DDoS).



Cloud migration.

Ransomware, the pandemic, and business change have led to more assets being moved to the cloud. Access controls are increasingly important.



Boards are not bored.

Oversight expectations have increased, and they're asking more questions. The board's responsibility is oversight, not management.



Out with the old. It's not enough to have data retention policies; you have to enforce them.



CPRA. It's coming. Are you ready?



You're only as strong as your weakest (vendor) link.

Vendor and supply-chain incidents continued and show why a good vendor-management program is necessary.



Wait, HIPAA applies to me?

If your company sponsors a group health plan, participant information is likely covered by HIPAA, and if such data is subject to unauthorized access or acquisition, you may have HIPAA notification obligations.



Beware of fraudulent fund transfer schemes –

e-crime adapts. Wire transfer / ACH / account takeover fraud exploded after states shut down fraudulent unemployment filing schemes.



Regulators are focusing more on ransomware attacks.

From the White House to state attorneys general, government entities and regulators are paying more attention to ransomware incidents. Some regulators are asking pointed questions about ransom demands and payments, and all are asking about what safeguards were in place when incidents occurred.

CONTENTS

02	At a Glance
04	Industries Affected
05	Incident Response Life Cycle
06	Deeper Dive into the Data
08	Forensics
09	Vendor Incidents Continue
10	Fraudulent Fund Transfer Incidents Persist

12	Data Breach Litigation Trends
14	Increased Regulatory Scrutiny of Cybersecurity Incidents
15	State and State Insurance Data Security Laws
16	HIPAA Update
18	Global Privacy

20	International Breach Notifications
21	Advertising, Marketing and Digital Media
22	CCPA Enforcement & CPRA Compliance
24	NFTs

Welcome to our 8th Annual Data Security Incident Response (DSIR) Report. What a year it has been!

2021 did not turn out the way many of us had hoped. Best-laid plans to “return to normal” were postponed numerous times due to multiple waves of COVID-19 outbreaks and new variants. The steady frequency of ransomware attacks in 2020 continued into 2021, highlighting the serious ongoing threat cyberattacks pose. The most frequent client requests this year included assistance with the ransom “pay-no pay” decision tree, OFAC compliance, and ransomware playbooks. The war in Ukraine and the responsive government sanctions have already increased interest in these topics, and we expect that to continue through 2022.

Despite these challenges, our clients continue to be resilient and more strategic in their approach to security than in the past. Clients are taking time to understand the best steps to secure their networks, and are relying on the information learned from others’ mistakes to guide their approach. Most significantly, perhaps, clients are becoming more nimble in their approach because of the constant evolution of technology and the legal landscape.

The Digital Assets and Data Management (DADM) Practice Group is in its third year of existence at the firm. The pandemic time warp we have been in makes it seem like we have been in existence forever — and that is because the seven teams that comprise the practice group work so well together to support our clients’ interests in the data life cycle. We now have several clients who utilize all seven teams to support their enterprise risk. Although the focus of this Report remains consistent with prior years, we have continued to broaden the topics and analysis to address the issues that the seven practice teams focus on: incident response, healthcare privacy compliance, global privacy issues, blockchain technology, non-fungible tokens (NFTs), truth in advertising, and emerging regulatory trends. We are excited to soon launch a new digital platform version of the DSIR Report that we plan to update throughout the year with real-time data to help keep you informed of trends.

Last year, I addressed the firm’s diversity, equity, and inclusion (DEI) efforts. One reader questioned why this topic was included in this Report. Let’s be clear: while conversations around DEI may be uncomfortable, they must occur. Being open about our efforts promotes conversations both inside and outside of our organization — that’s the way we improve and do better. In 2021, BakerHostetler announced it is participating in the Mansfield Rule 5.0 Certification process. The goal of the Mansfield Rule is to boost the representation of historically underrepresented lawyers in law firm leadership. Under the Mansfield Rule, BakerHostetler will commit to tracking and measuring that we have affirmatively considered at least 30% women, lawyers from underrepresented racial and ethnic groups, lawyers with disabilities, and LGBTQ+ lawyers for top leadership roles, senior-level lateral hiring, promotions into the equity partnership, and participation in client pitch meetings. The DADM Group continues to lead the way in this initiative. Currently, over 50% of our practice group is comprised of female lawyers and approximately 30% are persons of color or LGBTQ+. Our work is not finished and we intend to continue our efforts to attract, retain, and find a successful path upward for underrepresented minority groups.

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

1,270+

Incidents in 2021



**U.S. Breach
Notification Law
Interactive Map**

bakerlaw.com/BreachNotificationLawMap



**EU GDPR
Data Breach
Notification
Resource Map**

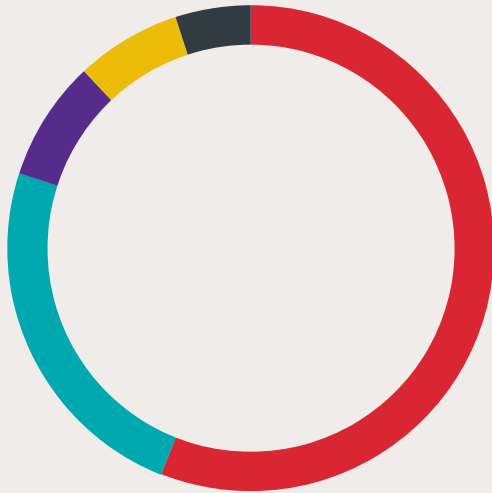
bakerlaw.com/EUGDPRResourceMap

For the latest, visit our blog

bakerdatacounsel.com

Incident Response Trends

Top 5 Causes



56%
Network Intrusion

24%
Phishing

8%
Inadvertent Disclosure

7%
System Misconfiguration/
Accessible Cloud Asset

5%
Stolen/Lost Devices
or Records

What Happens Next

37%
Ransomware

27%
Theft of Data

21%
Office 365 Account Access

17%
Installation of Malware

10%
Wire Transfer

2%
Cryptomining

1%
Espionage

Incident Response Timeline (median)

13

Days

Occurrence to Discovery

0

Days

Discovery to Containment

30

Days

Time to Complete Forensic
Investigation

59

Days

Discovery to Notification

Industries Affected



23%

Healthcare
(including Biotech & Pharma)

15%

Finance & Insurance

6%

Government

12%

Education

4%

Nonprofit

17%

Business & Professional Services
(including Engineering & Transportation)

10%

Manufacturing

2%

Technology

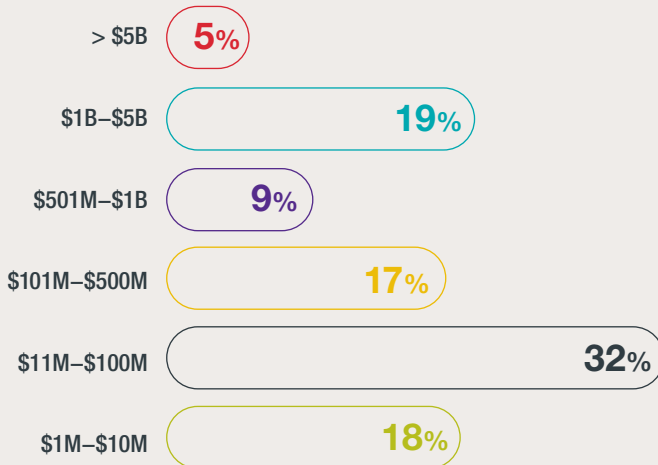
9%

Retail, Restaurant & Hospitality

2%

Energy

Entity Size by Revenue



> \$5B **5%**

\$1B–\$5B **19%**

\$501M–\$1B **9%**

\$101M–\$500M **17%**

\$11M–\$100M **32%**

\$1M–\$10M **18%**

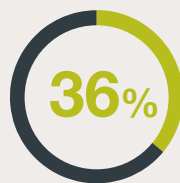
Average Forensic Investigation Costs

\$56,728 All Incidents

\$74,554 Network Intrusion Incidents

\$445,926 20 Largest Network Intrusion Incidents

Regulatory Inquiries Following Notification

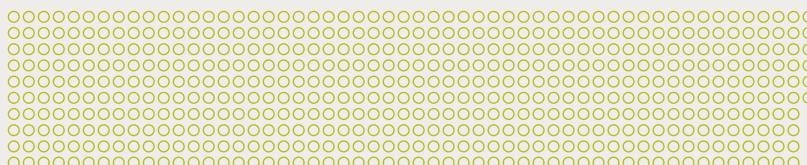


Average Ransom Paid

\$511,957

Notifications vs. Lawsuits Filed

536
Notifications



23
Incidents Resulted in Lawsuits



INDUSTRIES AFFECTED

AVERAGE

INITIAL RANSOM DEMAND	RANSOM PAID	DAYS TO ACCEPTABLE RESTORATION	FORENSIC INVESTIGATION COST	INDIVIDUALS NOTIFIED
-----------------------	-------------	--------------------------------	-----------------------------	----------------------

Healthcare

\$8,329,520 (median: \$1,043,480)	\$875,784 (median: \$500,846)	6.1 (median: 0)	\$62,724 (median: \$28,000)	81,679 (median: 1,002)
---	---	---------------------------	---------------------------------------	----------------------------------

Financial Services

\$3,064,559 (median: \$1,000,000)	\$513,928 (median: \$250,000)	12.8 (median: 5)	\$39,380 (median: \$15,000)	64,795 (median: 837)
---	---	----------------------------	---------------------------------------	--------------------------------

Retail, Restaurant, & Hospitality

\$3,032,936 (median: \$1,100,000)	\$351,986 (median: \$137,500)	7.8 (median: 7)	\$90,192 (median: \$46,625)	85,036 (median: 456)
---	---	---------------------------	---------------------------------------	--------------------------------

Manufacturing

\$2,362,636 (median: \$1,000,000)	\$593,993 (median: \$283,500)	10.2 (median: 5)	\$49,304 (median: \$32,000)	1,854 (median: 784)
---	---	----------------------------	---------------------------------------	-------------------------------

Education

\$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)
---	---	----------------------------	---------------------------------------	----------------------------------

Business & Professional Services

\$1,383,704 (median: \$409,800)	\$342,370 (median: \$120,892)	10.8 (median: 7)	\$42,815 (median: \$27,102)	9,131 (median: 361)
---	---	----------------------------	---------------------------------------	-------------------------------

Energy & Technology

\$9,553,333 (median: \$10,400,000)	\$3,000,000 (median: \$2,000,000)	4.6 (median: 2)	\$99,358 (median: \$53,000)	21,096 (median: 426)
--	---	---------------------------	---------------------------------------	--------------------------------

Government

\$764,500 (median: \$450,000)	\$142,122 (median: \$105,000)	11.5 (median: 10)	\$44,704 (median: \$36,500)	12,985 (median: 174)
---	---	-----------------------------	---------------------------------------	--------------------------------

INCIDENT RESPONSE LIFE CYCLE

Detection

Occurrence to Discovery

MEDIAN



AVERAGE

ALL INCIDENTS

84 Days

NETWORK INTRUSION

66 Days

Containment

Discovery to Containment

MEDIAN



AVERAGE

ALL INCIDENTS

5 Days

NETWORK INTRUSION

4 Days

Analysis

Time to Complete Forensic Investigation

MEDIAN



AVERAGE

ALL INCIDENTS

38 Days

NETWORK INTRUSION

41 Days

Notification

Discovery to Notification

MEDIAN



AVERAGE

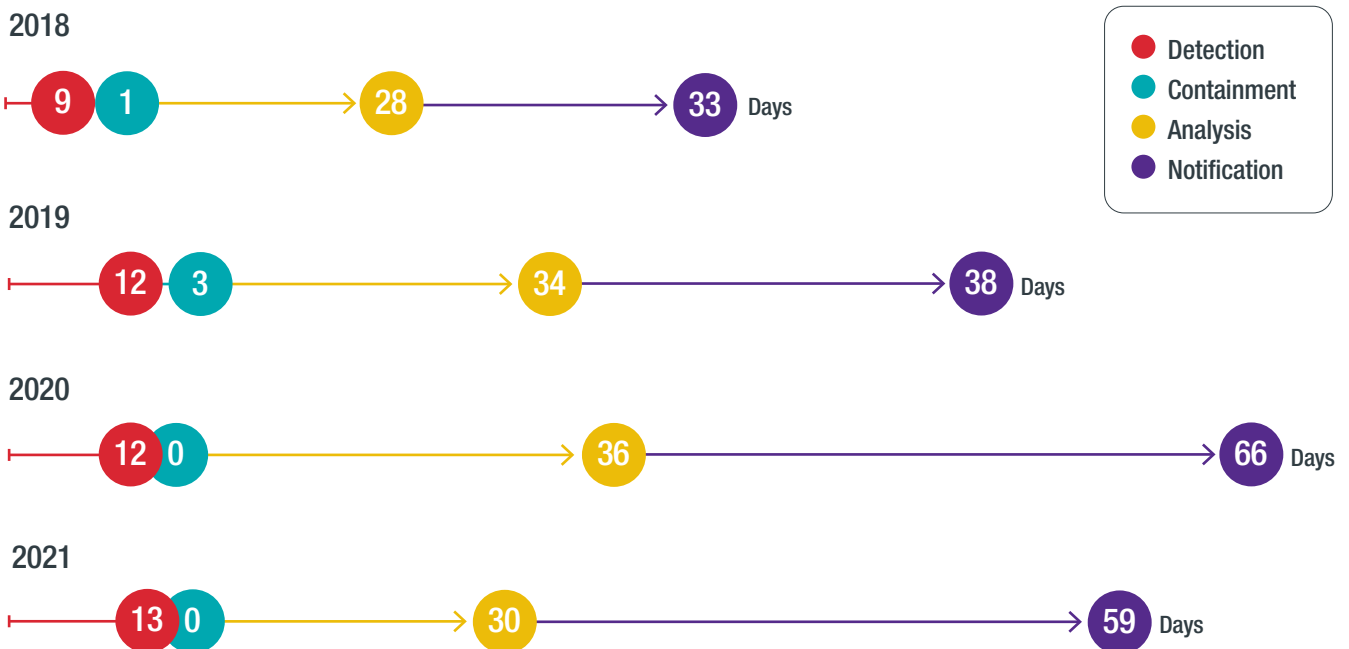
ALL INCIDENTS

74 Days

NETWORK INTRUSION

72 Days

Response Timeline (median data)



Ransomware Front and Center

2021 proved that ransomware isn't going away. Continued attacks and several high-profile incidents have drawn increased attention to the issue by government entities and regulators. Below are some observations and insights from the matters we handled in 2021, as well as critical actions organizations can – and should – take to prevent attacks and mitigate their effects if they do occur.

Ransomware Continues to Grow

Ransomware now represents 37% of the matters we handle, compared to 27% in 2020. In healthcare matters, ransomware represents 35% of the matters we handle, compared to 20% in 2020. Companies should accelerate their efforts to put effective mitigation measures in place. These include multi-factor authentication (MFA), endpoint detection and response tools, patch management protocols, and robust backup plans.

37% of total matters involved ransomware

35% of healthcare matters involved ransomware

Trying to Isolate Their Victims

Several ransomware groups threatened to cut off communications, delete decryption keys, and immediately publish data if companies engaged third-party ransom negotiators or law enforcement. Some threat actors have even asked companies to identify the specific employee at the company who is communicating with them. They then call the employee and demand that they read back the most recent chat as proof that a third-party ransom negotiator is not involved. Engaging advisors with the most up-to-date information about threat actors' tactics is key to avoiding pitfalls.

80+
threat actor groups/variants
(75 in 2020; 15 in 2019)

PYSA/Mespinoza Sodinokibi
MountLocker Ryuk

Additional OFAC Due Diligence

Following the U.S. Treasury Department's September 2021 supplemental guidance on the Office of Foreign Assets Control (OFAC) considerations for ransom payments, some insurance carriers and banks have expanded the list of due diligence questions they will ask a company to answer before facilitating a wire transfer for a ransom payment or providing reimbursement. Make sure to engage with these partners early in the process. Understanding their requirements will help avoid unnecessary delays in paying a ransom. Taking the appropriate steps to confirm that the recipient of the payment does not have a known sanctions nexus remains vital as well.



Longer Negotiation Timelines Lead to Smaller Payments

Of the ransomware matters we helped manage in 2021, the average ransom demand paid was around \$511,957, roughly two-thirds the average amount paid in 2020. Over the same time period, the median time between demand and payment was eight days compared to five days in 2020. This is likely a driving factor in the decrease in the average ransom demand paid. More organizations have invested in improving their data backup capabilities and are able to continue at least partial operations after a ransomware incident, which puts them in a better position to negotiate for a longer period of time and reach a greater discount for the ransom demand, if the need to pay arises. Also, if a decryptor tool is not needed and an organization is only paying to prevent further disclosure of their data, they can often take more time to negotiate the demand, which can lead to a deeper discount. Developing business continuity protocols and identifying workarounds for critical business operations — prior to an incident — are key to placing organizations in the strongest position if they experience a ransomware incident.

\$60+
million

Largest ransom demand in 2021
(2020 was \$65+ million)

\$5.5
million

Largest ransom paid in 2021
(one variant was involved in six of the
10 largest 2021 payments)

\$511,957

Average ransom paid in 2021
(2020 was \$794,620)

11.1

Days

From demand to payment
(median: 8)

9.8

Days

From demand to payment for
payments over \$1 million
(median: 8)

13

Days

From demand to payment for
payments \$200,000–\$1 million
(median: 10)

12.2

Days

From encryption to restoration
(median: 9)

Exfiltration of Data Is the ‘New Normal’

What was once rare has become an unfortunately common tactic threat actors use to exert pressure on victims to pay ransom demands. Claiming to have stolen data gives threat actors another piece of leverage to obtain a ransom payment. Even a victim that does not need a decryption key might still pay to prevent the public release of data.

In our 2021 ransomware matters, threat actors claimed to have stolen data 82% of the time. This is compared to 70% of the time in 2020, a continuation of a trend that we started to see that year. In healthcare ransomware matters, the percentage is even higher: 89% of the time, threat actors claim to have stolen data as compared to 79% in 2020. Encryption and good data hygiene are critical to avoiding theft of sensitive data that could lead to notification obligations, regulatory scrutiny, or even lawsuits. Having and following data retention policies, minimizing storage of documents with personal or proprietary information on file servers (common targets for threat actors looking for large amounts of data to steal), and avoiding use of personal information, such as Social Security numbers, where possible, are all steps that organizations can take to mitigate the risk and potential impact of data exfiltration.

80% of the time an organization was able to partially or fully restore from backup without paying ransom

81% involved theft of data resulting in notice to individuals

82% of ransom notes contained claim of theft of data before encryption

24% of matters involved a payment to a threat actor group even though the organization had fully restored from backup

73% found evidence of data exfiltration when there was a claim of data theft in the ransom note

33% paid even though the organization was able to partially restore from backups

FORENSICS

Many organizations have taken steps to proactively implement enhanced security tools. These investments have paid off, as our year-over-year statistics reflect.

Specifically, the median number of days between intrusion and detection in 2021 was nearly half what it was in 2020. Organizations are detecting intrusions more quickly and many threat actors are no longer lingering in systems before accomplishing their objectives. Threat actors don't want to be detected and kicked out, so they are shortening their own dwell times. Additionally, the notification timeline is trending down due in part because threat actors are more quickly providing information about the data they stole. This then informs the forensic investigation, which can focus on the systems from which the data came, giving a better and earlier understanding about the data involved, thus enabling earlier notification timelines.

Average Forensic Investigation Costs

\$56,728

All Incidents

\$74,554

Network Intrusion Incidents

\$445,926

20 Largest Network Intrusion Incidents

Network Intrusion Timeline (median data)

2019



2020



2021



- Detection
- Containment
- Analysis
- Notification

VENDOR INCIDENTS CONTINUE

19% of total incidents involved vendor causes

55% of vendor-caused incidents had notice requirements

10% of notices had regulatory inquiries

Third-Party Service Providers

Elekta **Kronos** **Vertafore**
LogixHealth **benefitexpress**
EyeCare Leaders **CaptureRX**

Vendor-caused incidents surged in 2021 as an increasing amount of sensitive data flowed to third parties. As we learned from some of the high-profile vendor incidents in 2020, these attacks have widespread impacts and lasting effects. In 2021, this trend continued with compromises of third-party service providers, including benefitexpress, CaptureRx, Elekta, EyeCare Leaders, Kronos, LogixHealth, and Vertafore. The nature of the services these third parties provide and the troves of data they maintain make them high-value targets for

threat actors. The importance of vendor risk management cannot be overstated.

Vendor-caused incidents present unique challenges to incident responders, who often are at the mercy of their vendor's decisions and willingness to share information. These incidents have varying degrees of operational and financial impact on companies, based on their unique relationships with their vendors. Below are some lessons learned and tips for strengthening defenses around vendor-caused incidents.



Discovery and Notification Timelines Vary Greatly The time it takes vendors to notify their customers of an incident can vary greatly depending on the type and extent of the incident, the scope of the vendor's services, and the parties' legal or regulatory obligations. This often leads to a longer notice timeline to individuals.



Information Sharing Also Varies Because the incident occurred at the vendor, the vendor controls the investigation, as well as what information is shared with customers and when. Even after completion of the investigation, vendors may be unwilling to share full details, which is often frustrating to customers.



Vendor Vetting (and Re-Vetting) Remains Key Before engaging a new vendor that will receive access to their environment or data, customers must exercise due diligence to make sure the vendor has adequate security safeguards in place. Ongoing vendor diligence is also critical to help prevent an incident involving their data.



Understand and Limit Data Sharing On both the customer and vendor side, minimizing the personal and/or sensitive information shared with or accessed by a vendor can mitigate risk and exposure.



Make Notice Provisions Make Sense Customers often try to add urgency to vendor breach notification obligations through contract language (e.g., "immediately," "within 24 hours," "within 72 hours"). However, as incident responders know, upon discovery, there is little meaningful information available, and downstream contracts are often not top of mind. It's important to strike a balance between a desire for transparency and the realities of breach response to ensure the notice customers receive is useful and actionable. This is especially important for highly regulated organizations, like healthcare providers and financial institutions, as vendor incident notifications could "start the clock" on their legal breach notification deadlines, which could be problematic if the scope of the incident and data involved is not yet known.



Know Your Remedies When an incident involves thousands of customers, the language in the vendor contract is critical to determining customers' rights.



Customers Face Regulatory Scrutiny and Class Actions Too Despite incidents occurring at the vendor, we do see regulatory investigations and class actions against downstream customers.

FRAUDULENT FUND TRANSFER INCIDENTS PERSIST

Beginning in 2020, we saw an increase in the number of phishing and social engineering attacks that attempted to divert, or successfully diverted, wire transfers, direct deposits, and Automated Clearing House (ACH) payments. The prevalence of incidents involving fraudulent fund transfers continued in 2021.

Reasons Cited by Law Enforcement for the Increase in Fraudulent Fund Transfer Incidents

- **Use of Stolen Data from Ransomware Attacks to Commit Fraud.** Law enforcement reports suggest that threat actors are using data they have exfiltrated through ransomware attacks to manipulate legitimate emails and invoices. These are used to obtain funds through fraudulent wire transfers, often using “spoofed” email addresses for legitimate email addresses. Because the threat actors have a treasure trove of stolen data to work with, they often do not need to access the email accounts of legitimate parties to the financial transaction. When victims do not address the vulnerability that led to the ransomware attack, the threat actors can persist in their environment and leverage that access to gain more information to use for fraudulent activities.
- **Pivot to Fraudulent Fund Transfers for ‘Easy Money.’** Some threat actor groups that traditionally engaged in ransomware attacks appear to be pivoting to fraudulent fund transfer schemes and business email compromises. This involves unauthorized access to email accounts, usually through phishing emails. According to law enforcement, fraudulent fund transfers and business email compromises can sometimes have a quicker “return on investment” than ransomware attacks, which may be attracting threat actors to these types of crimes.
- **Taking Advantage of Remote Work Environment to Commit Fraud.** Threat actors used the work-from-home environment arising from the COVID-19 pandemic to their advantage to commit fraudulent fund transfers. Especially at the beginning of the pandemic, many people were not used to working from home, which made them more vulnerable to fraudulent fund transfer schemes.

Fewer ‘Successful’ Fraudulent Fund Transfers

Our clients were able to identify fraudulent fund schemes *before* transferring funds more frequently in 2021 than in 2020. In fact, in 2021, 40% of clients identified fraudulent fund transfer schemes before any loss of funds, as compared to just 30% in 2020.

This trend likely results from more employee education and training on direct deposit, wire transfer, and ACH payment protocols, and on identifying potential fraudulent fund transfer schemes before losses occur.

More Fraudulent Fund Transfer Incidents Triggered Legal Breach Notification Requirements

What if a company recognizes that a fund transfer request is fraudulent and does not complete the transaction? The company should still conduct an internal investigation to determine whether the incident involved a business email compromise. In many instances, perpetrators of fraudulent fund transfer schemes are not interested in stealing personal information stored in email accounts, but the incident could still trigger notification obligations under federal and state breach notification laws if such information was or could have been accessed or acquired as a result of business email compromises.

In fact, in 2021, 60% of the fraudulent fund transfer incidents we advised clients on involved business email compromises that triggered breach notification obligations, as opposed to just 43% in 2020.

Business email compromises related to fraudulent fund transfer incidents are increasing. This may stem from companies not providing enough training on how to use MFA for email access. Or companies may be failing to implement MFA technology on their email tenants that could decrease the number of business email compromises. In some instances, companies did not enable certain types of logging in their email tenants. Thus, they cannot rule out the possibility that a business email compromise may have resulted in unauthorized access to personal information, triggering requirements to notify individuals and regulators.

Recovery Rate Increased

In 2021, funds involved in fraudulent fund transfer schemes were recovered 43% of the time, up from the 38% recovery rate we saw in 2020.

These trends are likely the result of more awareness among companies and employees about fraudulent transfer schemes, which may have shortened the time it takes to identify incidents and report them to banks and other authorities. Increased efforts from federal law enforcement agencies to help companies recover lost funds have also contributed.

\$48 million

In fraudulent wire transfers

\$743,106

Average wire transfer

\$166,257

Median wire transfer

\$12 million

Largest wire transfer

\$10.2 million

Second-largest wire transfer

\$890,135

Average recovery

\$181,577

Median recovery

43%

Matters that had recovered funds (totaling over \$24 million combined)

Top Five Tips to Prevent Fraudulent Transfers

These steps may help your company prevent fraudulent transfer incidents:

- 1 Use MFA** for remote access to online accounts, including email and payroll portals, and disable legacy authentication in your email tenant.
- 2 Train employees** regarding phishing emails and common fraudulent fund transfer schemes.
- 3 Establish written policies and procedures** related to authorization and approval of changes to wire transfer, ACH payment, and direct deposit information.
- 4 Design contract provisions** with vendors and customers that require in-person or voice authentication for changes to existing wire transfer, ACH payment, and direct deposit information.
- 5 Research** if something seems awry, look up the telephone number that you have on file for the email sender (not the contact listed in their email), and call the sender to confirm that what is being requested is legitimate.

What to Do if Your Company or a Vendor Loses Funds as a Result of a Fraudulent Fund Transfer

If your company or a vendor loses funds as a result of a fraudulent fund transfer, BakerHostetler recommends that you:



Notify the bank immediately

- If the fraud involves a wire transfer, the payor in the transaction should *immediately* contact their bank and ask them to initiate a “SWIFT recall” on the wire transfer and contact the fraud department of the receiving bank so it can freeze the funds in the recipient account.
- If the fraud involves an ACH payment, the payor in the transaction should notify their bank of the fraud and ask their bank to initiate an ACH payment reversal.



Retain legal counsel and contact law enforcement

- Engage legal counsel to contact law enforcement and to provide guidance on how to respond to the incident.



Conduct an investigation

- If it is determined that the fraud involved unauthorized access to your email tenant, have legal counsel retain a forensic firm to assist with the investigation. They can help determine if the incident resulted in unauthorized access to emails or attachments containing information that triggers legal or contractual breach notification obligations.

DATA BREACH LITIGATION TRENDS

More class action lawsuits are filed per incident

In 2021, there was a trend of multiple lawsuits being filed in the same venue within weeks following incident notification, even for smaller incidents. Previously, there was always a risk of multidistrict litigation following large data incidents. However, now we are seeing multiple lawsuits following an incident notification in the same federal forum. Or, in the alternative, we see a handful of cases in one federal forum and another handful of cases in a state venue. This duplicative litigation trend is increasing the “race to the courthouse” filings and increasing the initial litigation defense costs and the ultimate cost of settlement, due to the number of plaintiffs’ attorneys involved.

Plaintiffs’ Bar Cooperating Less

In 2021, we saw distrust and an unwillingness to cooperate among the plaintiffs’ lawyers litigating privacy cases, especially in duplicative class actions. This means that there have been fewer voluntary consolidations and more challenged motions for the appointment of leadership by the courts. As a corollary, we are also seeing a trend of courts no longer appointing a large cast for leadership (e.g., fewer committee appointments, fewer liaison counsel, etc.). A recent example involved a matter we are defending with three federal cases filed in the same district and six state cases. In the federal court, the judge consolidated the three actions but rejected an uncontested motion to appoint multiple lawyers as interim lead counsel and appointed only one. In the state court action, the court permitted consolidation of the currently filed six state court actions but refused to consolidate any future-filed class actions. That state court also permitted only a few of the proposed counsel to take leadership positions for the putative class, rejecting alternatives that increase the leadership committee structure, and in turn, defense costs.

Using the First-to-File Doctrine and Similar Procedural Tactics to Limit Increased Exposure from Multiple Filings in the Same Venue

In response to the trends of increased filings per incident, our team is working on new ways to limit the additional exposure caused by multiple filings and uncooperative plaintiffs’ counsel. For example, in some circumstances, we are working to limit consolidation even in the same venue, asking the court to stay duplicative actions in the same venue instead of consolidating them. In other circumstances, our team is working to oppose efforts that increase the number of interim lead counsel. Both strategies can be effective at reducing both litigation defense costs and any settlement exposure.

Class Certification Jurisprudence in Data Breach Litigation Comes into Focus

Over the past decade, there have been very few published class certification rulings following data incidents, but the majority that existed were favorable to the defense. However, 2020 and 2021 brought two critical class certification rulings that are emboldening plaintiffs’ firms, in both the number of their litigation filings and their negotiation tactics during mediations. In April 2021, a court certified a class of individuals whose payment card information had been compromised. *In re Brinker Data Incident Litig.*, 2021 WL 1405508, at *1 (M.D. Fla. Apr. 14, 2021). There, the defendant argued that the plaintiffs could not prove causation because at least one named plaintiff had been involved in a previous breach. The court found that this “multiple breach issue” is “not a disqualifying causation issue, but rather to be determined at the damages phase.” *Id.* at *12. Additionally, the court rejected the defendant’s argument that differences in damages predominated over any common issues, finding that Plaintiffs’ expert had offered “a common method of calculating damages that allows the Court to determine individual class members’ damages in a non-complex and non-burdensome way.” *Id.* Based on these findings, the court certified a nationwide class for the plaintiffs’ negligence claim and a California-only subclass for plaintiffs’ unfair competition claims. We predict that this same reasoning will not be applied to non-payment card cases, but its holding will need to be considered in any litigation strategy, as long as it remains good law.

Although *Brinker* may be an outlier, in 2020, one court certified an injunctive relief-only* class but denied certification of all damages. *Fero v. Excellus Health Plan, Inc.*, 502 F. Supp. 3d 724, 746 (W.D.N.Y. 2020). The outcome in *Excellus* mirrors an earlier decision by the Northern District of California, *Adkins v. Facebook*, 424 F. Supp. 3d 686, 698 (N.D. Cal. 2019). Ultimately, certification of only injunctive claims can be a hollow victory for plaintiffs because it eliminates the possibility of a large monetary judgment and because most defendants who have suffered a data breach will have made significant changes to their data security posture by the time the case gets to trial.

* A class that is certified for injunctive relief only is only entitled to compel the defendant to take or stop taking certain actions. It is not entitled to any monetary damages.

Incident Response Mailing Statistics Impact CAFA Jurisdiction

Litigation is often dictated by the raw numbers of persons notified in an incident. However, the mailing statistics for that population are increasingly impacting the venue decisions for defendants. For example, in some circumstances, our team has secured a favorable federal court forum despite over 85% mailing addresses being in one state. There, our team argued that mailing addresses are not dispositive of citizenship, the court could not use undeliverable addresses as evidence of residency, many of the deliverable addresses were intrinsically transitory (nursing homes, homeless shelters, universities, etc.), and therefore there was no evidence of citizenship sufficient to satisfy the burdens of the U.S. Class Action Fairness Act of 2005 (CAFA)'s home state exceptions. In another circumstance, our team was able to secure a more favorable state court venue by seeking to dismiss duplicative federal court litigation based on lack of CAFA jurisdiction where 96% of mailing addresses were in one state.

Number of Incidents that Resulted in Lawsuits by Individuals Notified



23

incidents disclosed in 2021 resulted in one or more lawsuits filed (compared to 20 in 2020).

- **19** incidents involved SSNs
- **16** incidents involved medical/health information
- **5** incidents involved payment card data
- **3** incidents started with system misconfiguration
- **15** incidents involved ransomware
- **18** incidents started with network intrusion
- **4** incidents were vendor related

58+

total lawsuits filed related to the 23 incidents

- **8** incidents had more than one (but less than 5) lawsuits filed
- **4** incidents had five or more lawsuits filed
- **43** lawsuits were against a healthcare organization

INCREASED REGULATORY SCRUTINY OF CYBERSECURITY INCIDENTS

In the wake of the 2020 SolarWinds and 2021 Colonial Pipeline cyberattacks, the federal government enacted new laws and focused more on cybersecurity incidents.

Executive Branch

President Biden issued the Executive Order on Improving the Nation's Cybersecurity, which directs federal agencies to take steps to improve the federal government's ability to identify, protect against, detect, and respond to cybersecurity threats.

Securities and Exchange Commission

Eight organizations were sanctioned for failures in cybersecurity policies and procedures.

Over 100 entities were asked to voluntarily provide information about the impact SolarWinds may have had on their businesses and whether any required disclosures in connection with the incident or unrelated "Other Compromises" were required.

Office of the Comptroller of the Currency

The Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation, and Federal Reserve Board implemented a joint rule regarding computer-security incident notifications, which went into effect on April 1, 2022, with a full compliance date of May 1, 2022.

The rule applies to banking organizations and their bank service providers.

Notification requirements focus on incidents that disrupt or affect bank operations, not just situations where customer data is accessed or acquired, which are referred to in the new law as "notification incidents."

The rule requires covered organizations to notify their primary federal regulator "as soon as possible and no later than 36 hours" after an incident is discovered. Bank service providers must notify their banking organization customers when they experience an incident.

In light of the new rule, banking organizations and banking service providers need to update their incident response plans to include determining if notice to a banking organization or primary federal regulator under the rule is required.

FinCEN

In November 2021, the Financial Crimes Enforcement Network (FinCEN) issued Advisory FIN-2021-A004, related to the use of the financial system to facilitate payments to ransomware threat actors.

The main takeaway from the Advisory is banks, insurance companies, money services businesses (MSBs), and other entities subject to the Bank Secrecy Act (BSA) should file a suspicious activity report (commonly called a SAR) if they think a ransomware payment is processed through them, including if they are involved in making such a payment to respond to their own incident.

FinCEN indicates that entities engaged in money transmission must register as MSBs with FinCEN and are required to file a SAR when facilitating a ransomware payment. FinCEN is using this data to track the activities of the different ransomware groups and to quantify the ransoms they are able to extract. For example, it noted that two ransomware variants, Darkside and Sodinokibi/REvil, which were behind the Colonial Pipeline and the JBS and Kaseya attacks, respectively, were among the costliest variants in the first half of 2021, accounting for 458 reported ransomware-related transactions with a total value of \$590 million.

Forewarned Is Forearmed: Ransomware Due Diligence Requirements



In its November 2021 advisory, FinCEN included a list of "Financial Red Flag Indicators of Ransomware and Associated Payments" for financial institutions to use in identifying ransomware-related transactions that might require them to file a SAR. Following the OFAC advisories in October 2020 and September 2021, and the October 2020 and November 2021 advisories from FinCEN, we have seen heightened scrutiny from financial institutions and cyber insurance carriers who are asked to facilitate or reimburse ransomware payments. As a result, some clients are now proactively working with their banks and carriers to understand their due diligence requirements for ransomware payments and considering those requirements in their ransomware preparedness planning. These requirements will likely evolve as ransomware operators continue to change their tactics. Meanwhile, knowing what financial institutions currently require can save valuable time for organizations that find themselves in the difficult position of having to pay a ransom.

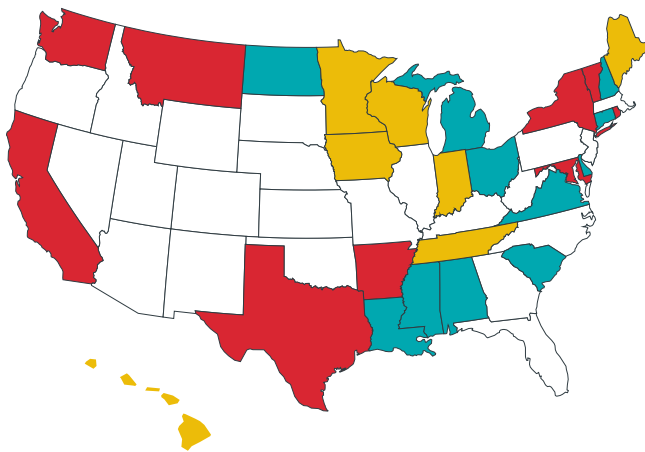
The federal government is likely using this information in its "whole-of-government" approach to combating ransomware. In November 2021, for example, OFAC sanctioned two individuals associated with Sodinokibi/REvil, noting that they were part of a cybercriminal group that "received more than \$200 million in ransom payments paid in Bitcoin and Monero." We anticipate that organizations involved in ransomware payments will continue to see increasing scrutiny from the federal government to report such incidents. Requiring a SAR is one way the government is gathering information about these incidents.

STATE AND STATE INSURANCE DATA SECURITY LAWS

This past year saw continued focus on cybersecurity incidents at both the federal and state levels for organizations in the insurance and financial services sectors. Additional data security laws were passed, and notice under those laws, and under regulatory guidance, is being required for more types of matters. Access to and/or acquisition of nonpublic information are not the only notification triggers, as they are under general state data breach notification laws. Licensees are also required to report incidents that are likely to materially harm their business, and regulators have made clear their expectation that network intrusions and ransomware events will often meet that standard. Entities involved in facilitating ransom payments also have increased federal reporting requirements.

More states continue to pass comprehensive data security laws for the insurance industry in response to the urging of the U.S. Treasury Department in 2017 to enact legislation or face congressional preemption. This past year, seven states adopted the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law or a variation of it—joining the 11 other states that had previously adopted it. Given

the strong recommendation by the Treasury Department for states to adopt such a law by 2022, more states will likely follow suit. Similar to the New York Department of Financial Services' (NYDFS) Cybersecurity Regulation, these laws include requirements for implementing and maintaining reasonable security practices as well as notification obligations in the event of a cybersecurity event.



-
- Newly adopted laws based on NAIC Model Law**
Hawaii, Indiana, Iowa, Maine, Minnesota, Tennessee, Wisconsin
-
- Previously enacted laws based on NAIC Model Law**
Alabama, Connecticut, Delaware, Louisiana, Michigan, Mississippi, New Hampshire, North Dakota (WISP requirements effective 8.1.22), Ohio, South Carolina, Virginia (WISP requirements effective 7.1.22)
-
- Enacted laws or provided guidance not based on NAIC Model Law**
Arkansas, California, Maryland, Montana, New York, Rhode Island, Texas, Vermont, Washington
-

State Insurance Department Hot Topics

► **Multi-Factor Authentication.** The hour is growing late for entities that haven't enabled MFA. Based on recently reported enforcement actions and our interactions with NYDFS in 2021, NYDFS requires most regulated entities to have MFA implemented where possible. Other state regulators are zeroing in on this issue, too. The Indiana Attorney General has started asking entities that report incidents whether they had MFA implemented at the time of the incident and, if not, to explain why. NYDFS and other regulators have increased their focus on companies' use of MFA and the specific authentication method utilized. In December 2021, NYDFS provided guidance to its regulated entities on MFA and stated that "not all forms of MFA are equal" and strongly encouraged the use of token-based MFA instead of push-based configurations, which NYDFS explained are more susceptible to human error.

► **Ransomware Attacks.** Given the number of high-profile ransomware incidents in 2021, we also saw some regulators clarify their reporting expectations for licensees who are confronted with ransomware. NYDFS issued updated guidance explaining that regulated companies should report "any successful deployment of ransomware on their internal networks" and "any intrusion where hackers gain access to privileged accounts." Even if nonpublic information was not accessed or exfiltrated, licensees may still have to report network intrusions and ransomware events. In many of the data requests and civil investigative demands we worked on, state departments of insurance asked for details related to ransomware incidents, including for copies of ransom notes and the ransom amount paid.

HIPAA at 25

HIPAA breaches of 500 or more individuals

2021 **714**

2020 **663**

2019 **512**

2018 **369**

2017 **358**

2016 **329**

Between the compliance date of the HIPAA Privacy Rule in April 2003 and 2021, there have been:

286,610

HIPAA complaints

1,105

Compliance reviews

275,145

Resolved complaints

29,354

Investigated and resolved cases

Increased Number of HIPAA Breaches Involving More than 500 Individuals

In 2021, OCR continued to investigate all breaches involving 500 or more individuals. In light of the increase in ransomware and vendor incidents as well as in those involving data exfiltration, the number of incidents involving 500 or more individuals has substantially increased over the years. According to OCR’s online portal, 714 incidents involving 500+ individuals were reported in 2021 — an increase of 51 from the year prior and an increase of 385 from just five years ago. Of note, 35% of the incidents involving 500 or more individuals reported in 2021 occurred at or by a Business Associate.

More OCR Referrals of Breach Investigations to the Department of Justice

More breach investigations involving criminal acts, such as ransomware and business email compromises, were

referred to the Department of Justice for possible criminal violations of HIPAA by OCR in 2021 than in years past.

Continued Focus on Individual Right of Access

- OCR continued to prioritize enforcing individuals’ Right of Access, which requires covered entities to provide patients or their personal representatives with timely access to their medical records at a reasonable cost.
- Of the 14 enforcement actions announced by OCR in 2021, 12 related to the individual Right of Access (bringing the total number to 25 since the initiative began in late 2019). Between 2019 and 2021, OCR obtained over \$1.5 million through the 25 right of access enforcement actions.
- Given the likelihood of this trend continuing, covered entities should at a minimum review their policies and procedures for providing records and ensure they are handled in a timely fashion.

Based on the resolution agreements related to alleged violations of the individual Right of Access requirements, here is a list of “red flags” that could prompt an OCR investigation:

- ▶ Taking more than 30 days to provide patients with the requested protected health information
- ▶ Incomplete records provided pursuant to patient access requests
- ▶ Lack of response to multiple access requests from the same patient
- ▶ Failure to provide records to a patient’s personal representative

From the first enforcement action in 2008 through the end of 2021:

2008

2021

105

Cases settled or issued a Civil Monetary Penalty by the OCR

\$16M

Highest amount paid as part of a resolution agreement

\$130M

Collected by the OCR through its enforcement actions

Uniqueness of Ransomware in Healthcare

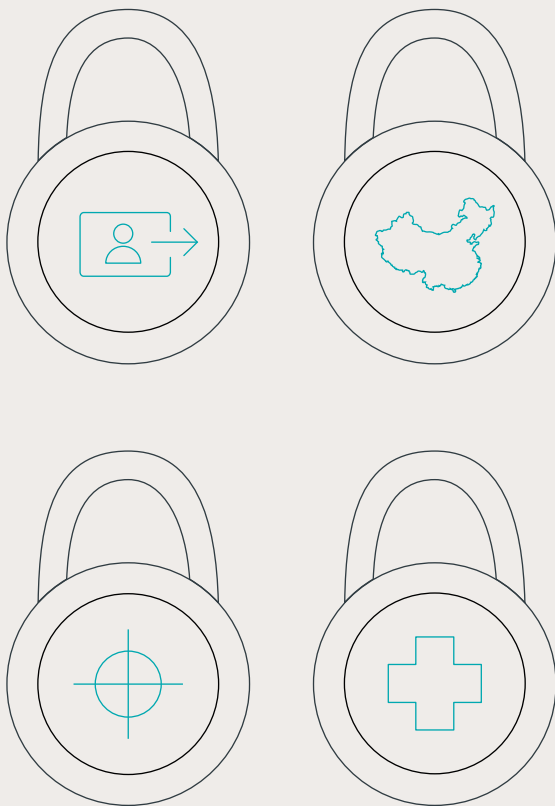
Ransomware incidents pose unique challenges to healthcare providers:

- **Operational disruptions create “life and death” situations.** When ransomware attacks make patient data and related systems inaccessible, healthcare providers have to quickly initiate unplanned, forced downtime procedures, including paper charting, and in some instances, the transfer of critical patients to other facilities, diversion of incoming ambulances, and procedure cancellations. These dire conditions leave healthcare organizations asking not whether they can, or want to, or should pay a ransom demand, but what is the quickest option to decrypt data and return to serving their communities.
- **HIPAA's definition of a breach increases likelihood of notification.** Unlike many state breach notification laws that are triggered by the acquisition of personal information, notification obligations under HIPAA are triggered by access to or acquisition of protected health information. In addition, per HHS guidance, data deletion or loss of data integrity due to a ransomware attack can also create notice obligations under HIPAA.
- **Lack of forensic evidence can lead to notification to entire patient populations.** Threat actors are extremely sophisticated and are regularly successful at stealing not just a few files but multiple terabytes of data and deleting forensic evidence to “cover their tracks.” Instead of spending the time and money to review each file purportedly accessed or acquired, a healthcare organization may be better off simply notifying their entire master patient index.
- **Ransomware attacks could jeopardize Medicare reimbursement.** In a striking departure from years past, in 2021, the Centers for Medicare & Medicaid Services began issuing blanket denials to Extraordinary Circumstances Exceptions requests made by healthcare providers seeking extensions for CMS filing deadlines due to ransomware attacks that limited access to their systems and data. The reason cited by CMS for these denials? The providers “could have feasibly received information describing how to prevent the occurrence of the cyberattack and did not address the risks in a complete and timely fashion.” This, despite the fact that CMS never asked the providers whether they were in possession of such information. These denials could result in a significant loss of Medicare reimbursement to healthcare providers that are already reeling from the toll the COVID-19 pandemic has taken on their finances. This new trend emphasizes the need for healthcare providers to quickly identify important, upcoming regulatory filing deadlines if there is a concern that a data security incident will prevent them from accessing the required information for the filing.

Heightened Attention to ‘Recognized Security Practices’

- A January 2021 amendment to the Health Information Technology for Economic and Clinical Health Act (HITECH) essentially created a “HIPAA Safe Harbor” for organizations that have implemented “recognized security practices.”
- Examples of “recognized security practices” that would be deemed acceptable defenses under this law include the methodologies set forth in the National Institute of Standards and Technology Act and the Cybersecurity Act of 2015.
- The amendment requires that OCR consider whether an entity had “recognized security practices” in place a year prior to the incident as part of any determination regarding fines, audit results, or other remedies.
- While the HITECH amendment does not provide entities with total immunity from HIPAA enforcement, it does provide organizations with substantial incentives to establish or improve their cybersecurity programs. It also provides a chance to mitigate financial penalties and other negative regulatory actions that may result from a data breach or security incident.
- In 2021, during the course of the over 40 OCR investigations BakerHostetler worked on, the OCR frequently asked our clients to describe what “recognized security practices” were *in place a year prior* to the underlying incident.
- Healthcare organizations looking to build their HIPAA-safe harbor defensibility should start by assessing whether their current cybersecurity program/processes fit the definition of “recognized security practices” as set forth in the HITECH amendment. If needed, they should consider additional investments to further mature their information security posture so they can rely on this safe harbor.

Four International Data Protection Law Developments



1 European Personal Data Transfer Update

Cross-border data transfer issues have long been a concern for U.S. companies doing business with Europe, but developments in 2021 put additional pressures on transfers to the United States specifically.

- **New Standard Contractual Clauses (SCCs) for International Personal Data Transfers.**

In June 2021, the European Commission issued new SCCs for international personal data transfers, and the European Data Protection Board (EDPB) also published final recommendations on supplemental personal data transfer measures to be implemented in conjunction with the new SCCs. These recommended supplemental measures are likely to be required for many U.S. companies in order to meet the strict standards established by the Court of Justice of the European Union's *Schrems II* decision in July 2020. On September 27, 2021, all older versions of the SCCs were repealed, meaning that any new or renegotiated agreements must now use the new SCCs. Existing agreements relying on the previous SCCs must transition to the new SCCs by December 27, 2022. European data protection authorities (DPAs) continue to issue guidance, initiate audits of data transfer compliance, and take enforcement actions related to noncompliant data transfers, including ordering data transfers suspended.

- **EU Personal Data Flow to the United Kingdom and South Korea.** Also in 2021, the European Commission approved adequacy for the United Kingdom and South Korea, so now EU personal data can freely flow to those countries.

2 China's New Data Protection Laws

Although many countries issued new or revised data protection laws in 2021, China has had the spotlight. Last summer, China passed two new data protection laws — the Data Security Law (DSL) in effect since September 1, and the Personal Information Protection Law (PIPL) in effect since November 1.

- **DSL Applies to Entities Inside and Outside of China.** The DSL applies broadly to data use and data processing activities, including those that take place outside China when they could harm the interests of China or its citizens and businesses.
- **New Data Security Requirements Included in DSL.** The DSL outlines data security requirements tied to a data classification system that aims to safeguard data through comprehensive data security management, ongoing assessments, regulatory reporting, and effective risk monitoring and remediation.
- **PIPL Has Global Reach.** PIPL covers the processing of personal information of individuals located in China, including when that information is processed outside China, such as when providing goods and services in China or analyzing or assessing the behavior of individuals in China.
- **GDPR Inspired PIPL.** PIPL draws inspiration from the EU's General Data Protection Regulation (GDPR) and other similar data protection laws. However, certain PIPL requirements differ substantially from those of the GDPR. For example, PIPL requires discrete consent for specified personal information processing activities, including disclosure, cross-border transfer and sensitive personal information processing.

3 Cookies and Tracking Technologies

France's data protection authority has led the way on enforcement related to cookies and tracking technologies. It is proactively auditing companies active in France and handing out serious fines for violations of France's law implementing the EU's ePrivacy Directive. But the French regulators are not alone in prioritizing compliant use of online tracking technologies; we have seen a lot of new guidance in 2021, including from the Danish, Finnish, Italian, and Turkish DPAs. Several other DPAs have taken related enforcement actions, and privacy advocates have pushed for greater transparency and consumer control in the AdTech sector generally. China's regulators, too, have been routinely taking action against apps that collect excessive personal information from users. Companies using non-essential cookies and other tracking technologies should be on the lookout for growing compliance demands.

4 Health Data

The use of health data to respond effectively to the COVID-19 pandemic has raised many privacy concerns, resulting in a near-constant stream of new guidance from DPAs worldwide. The use of vaccine passports and collection of employee COVID-19 vaccination status have been heavily debated worldwide. To highlight two examples of regulatory guidance: the Italian DPA emphasized that the inherent imbalance in the employer-employee relationship means that consent cannot be the legal basis for processing vaccination-related personal data, and consequences may not be based on an employee's vaccination status. The Irish DPA's guidance states that the collection of employee vaccination data is likely to be unnecessary and excessive with no clear legal basis. The use of health data has continued to be a hot spot for proactive data protection authority audits, and individual complaints of alleged health data misuses have also resulted in a number of recent regulatory enforcement actions.

Five Tips to Help Meet Tight Notice Deadlines

In addition to the often-discussed 72-hour regulatory notification obligation of the GDPR, dozens of other countries worldwide require breach notifications to be made in a week or less. These include countries like South Korea that actively enforce data protection compliance. Many companies struggle to meet these requirements, and regulators are paying more attention to breach notification timing, and the reasons provided for delayed notices, in considering enforcement actions and calculating potential fines.

For example, in 2021, the Dutch DPA imposed a fine of €475,000 for failure to notify within 72 hours. The DPA found

the delay was in part due to a lack of internal processes that should have triggered appropriate investigations and escalations. In an Irish DPA decision, a company could not blame its delayed data breach notification on its processor's failure to provide timely notification to the company. According to the Irish DPA, the company needed to have its own processes in place to ensure data breaches were reported in a timely manner, including when data processing was outsourced, as processors remain under company oversight. These five tips can help you avoid unnecessary international data breach notification delays.

1. Know the international laws and regulatory authorities applicable to your company.

Analyzing international data breach notification obligations begins by identifying the relevant laws, which can involve multiple conversations with various business stakeholders. If a company has already assessed and documented the applicable foreign laws, it can use this analysis to move directly to evaluating whether data breach notification triggers have been met. Also, evaluate whether your company is subject to sector-specific obligations, such as those commonly relevant to critical infrastructure, health, finance, and telecommunications, as these often trigger separate reporting obligations to their own regulatory bodies. Identifying the appropriate laws and regulators in advance, including whether you have a lead supervisory authority in the EU, can give your breach response team a real advantage.

2. Recognize the types of personal data covered by each applicable foreign law.

If you have a data map and inventory, that's great! But not all companies do. At a minimum, you should understand whether particular types of personal information are sensitive. Many companies have grown used to relying on the special categories of data outlined in the GDPR, but other countries include different personal information as sensitive. Sensitive personal data often triggers data breach notification requirements, so knowing whether sensitive personal data is included in a data breach can help to identify notification obligations more quickly.

3. Clearly understand your company's global business profile and compliance posture.

Familiarity with where your company employs a large workforce, targets key markets, or has built regional headquarters will help to focus your breach response team on jurisdictions most likely to be in play. Additionally, appropriate people in the data breach response chain should be aware of the company's overall data protection compliance posture as well as prior regulatory interactions. For example, we see

regulators closing data breach matters with warnings regarding future data breaches or other perceived deficiencies that may need to be addressed in new notifications. It is also common for regulators to look into other aspects of a company's compliance program following a data breach notification, so it is important to understand a company's general compliance status before notifying regulators in each jurisdiction.

4. Have information commonly requested in notice forms readily available.

While much of the information required in notice forms is related to the specific data breach, notice may be delayed while other information that could have been gathered in advance is tracked down. Here is a quick list of information you should be prepared to provide:

- Full company name and address, including any relevant overseas entities
- Location of company headquarters and all other company establishments (including, if possible, processing activities and decision-making functions associated with each establishment)
- Business identification numbers or tax identification numbers
- Number of employees
- Frequency and completion information for employee data protection training sessions
- Name and contact details for the Data Protection Officer (or other key privacy contact)
- Brief description of preventative security measures currently in place

5. Account for translation time.

Depending on the availability of translators, which often decreases for less common languages, translation for regulatory notice can easily take 24-48 hours, and most regulators require notice in an official language recognized by the country.

Truth in Advertising Trends

At the NAD

The National Advertising Division (NAD) is the investigative unit of the advertising industry's system of self-regulation. It monitors national advertising and resolves disputes to increase consumer confidence in the truth and accuracy of advertising claims and to support fair competition. Overall, 2021 saw business as usual at the NAD. Key trends included:



increase in compliance cases



increase in telecom cases



increase in food and beverage cases



increase in financial services cases, mostly monitoring



decrease in referrals (4 in 2021 vs. 10 in 2020)



of all challenge cases were Fast-Track SWIFT cases*

New Types of Businesses with Cases Before the NAD

- Cord blood storage
- Ambulance services
- Diamonds
- Pet insurance
- Olive oil
- Tuna
- Security deposit insurance
- Automotive
- Grocery stores

* Single Well-Defined Issue Fast Track (SWIFT) is the fastest route to resolution offered by the NAD. SWIFT challenge cases only accounted for 6.5% of all cases, including monitoring, compliance, standard and complex.

At the FTC

The Federal Trade Commission (FTC) underwent significant changes in 2021, with new leadership and changes in its authority. The U.S. Supreme Court decision in *AMG Capital Management vs. FTC* struck down the agency's ability to use Section 13(b) of the FTC Act to seek monetary relief in federal court, a tool the agency had used for decades. The FTC also underwent two leadership transitions, with Commissioner Rebecca Slaughter becoming the Acting Chair in January 2021 and with Lina Khan becoming Chair in June. Chair Khan has emphasized an enforcement agenda focused on issues involving technology and healthcare and bringing more enforcement actions against larger industry players. Among the things we saw in 2021:

1,800

warning letters sent to companies threatening future civil penalty actions for violations (includes "Notices of Penalty Offenses")

31











new consumer protection complaints were filed by the FTC (in federal court and administratively)

68%

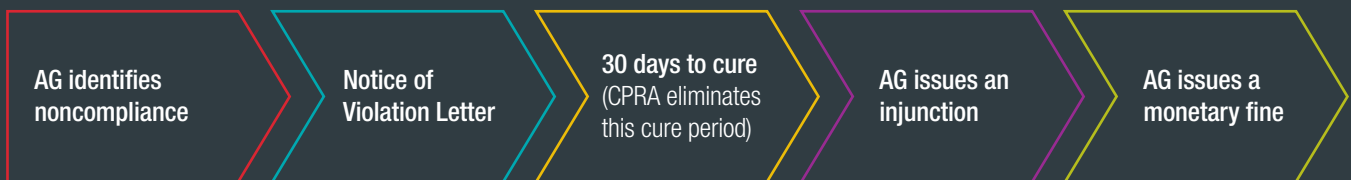
of the new complaints filed by the FTC named individuals as well as corporate entities

Overview of CCPA Enforcement

Since the California Consumer Privacy Act (CCPA) enforcement began in July 2020, the California Office of the Attorney General (OAG) has sent hundreds of Notice of Violation (NOV) letters and Requests for Information (RFI) to companies in a broad range of industries, including big tech, retail, advertising technology, telecommunications, financial services, and others. While these investigations and enforcement actions are confidential to date, the OAG has published a number of case examples to provide guidance on its enforcement priorities and how it is interpreting some of the CCPA requirements. In 2021, we assisted companies in responding to CCPA investigations by the OAG. The issues raised by these investigations included:

 <p>Privacy Notice Content, form, and tone of the notice required to be provided to consumers under the CCPA</p>	 <p>Offline Collection Notice Content and delivery method for offline notices, including Notice at Collection and Notice of Financial Incentive (NOFI)</p>	 <p>Sale Analysis of whether a “sale” under the CCPA occurs in the context of digital advertising</p>	 <p>Right to Opt-Out and Global Privacy Control (GPC) “Do Not Sell” button, cookie preference center, and GPC design and implementation</p>	 <p>Service Provider Contracts Service provider contract terms required under the CCPA and the obligation to flow down deletion requests</p>
 <p>Right to Know Content and format of how businesses should respond to consumers’ request to know</p>	 <p>Right to Delete Analysis of exemptions that apply to deletion rights, in particular related to the deletion of transaction history</p>	 <p>Right to Non-Discrimination Analysis of loyalty programs and discount offers from businesses and the application of the non-discrimination right</p>	 <p>Data Monetization and NOFI Opt-in consent requirement for NOFI and methods of calculating the value of the consumer data</p>	 <p>Metrics Record-keeping requirements and consumer response process metrics</p>

Attorney General Enforcement Path



CPRA Compliance

In 2021, companies started conducting gap assessments to identify compliance gaps using the CCPA enforcement examples and to begin preparing for the California Privacy Rights Act (CPRA), which goes into effect January 1, 2023. The CPRA amends and builds upon the compliance requirements under the CCPA. For example, the CPRA provides additional and expanded rights for consumers (and thus obligations for businesses), including the right to correct inaccurate personal information and the right to opt out of sharing for “cross-contextual behavioral advertising.” If the California legislature does not amend the CPRA prior to the January 1st effective date, the exemptions related to business-to-employee (B2E) and business-to-business (B2B) will expire, thus bringing the data collected in these contexts under the full scope of the CPRA. Further, the CPRA established the new California Privacy Protection Agency (CPPA), a first-of-its-kind state agency responsible for implementing and enforcing the law. Notably, the CPPA’s authority is in addition to civil enforcement by the OAG and the consumers’ private right of action.

27

OAG Case Examples

Related CCPA Rights

Know/Access	11
Deletion	11
Opt-Out	13
Non-Discrimination	7

Absent or Confusing Sale of Personal Information Disclosures

‘Do Not Sell’ Link Absent or Not Functional

No ‘Notice at Collection’

Non-Compliant Service Provider Contracts

Inadequate Request Methods for Authorized Agents

No Notice of Financial Incentive

Non-Compliant Opt-Out Process

Charging Fees for CCPA Requests

Lack of Toll-Free Number

Inadequate Request Methods

Non-Compliant Privacy Policy

Untimely Responses to CCPA Requests

NFTs

Non-fungible tokens (NFTs) experienced a meteoric rise in 2021, with up to \$44 billion in NFT sales over the year and approximately 28.6 million cryptocurrency wallets engaged in NFT transactions. But as the market for these digital assets expanded, so did the risk of security incidents and fraud.



\$44 billion

in NFT sales in 2021



28.6 million

cryptocurrency wallets engaged in
NFT transactions

What is an NFT?

A non-fungible token (NFT) is a one-of-a-kind digital asset created, stored, and transferred on a blockchain network, with ownership and transaction history recorded and verified on that network's blockchain (i.e., digital ledger). This means that the owner of an NFT can prove—without the need for a third-party intermediary—that they are the verified owner. Though typically used to display and transfer data referring and pointing to online digital media files, such as digital artwork, NFTs also have the potential to be used to represent actual ownership of any intellectual property associated with the digital files, as well as physical items, such as real estate. While fungible assets, much like a dollar bill, can be replaced or exchanged with another identical one of the same value, NFTs are unique, meaning no two NFTs are the same.

Social Engineering and Phishing Hacks

NFT projects often attract thousands of potential purchasers from around the globe, funneling users to online chat communities that aggregate information about the NFT launch date, price, and purchase links. These communities have become targets for scammers, who infiltrate the communities (often masked as community administrators) and deploy social engineering and phishing tactics that can enrich hackers to the tune of millions.

Hackers have identified intrinsic vulnerabilities in this model where buyers are often primed to move fast or risk missing out, and are flooding various NFT projects' chat servers with malicious links. The links, promising things like limited edition NFTs, entice users to connect their cryptocurrency wallets and thus allow hackers to steal associated funds.

Avoiding these types of incidents is tricky and currently requires project curators to exhibit excellent fan and customer communication. NFT community curators should be prepared well before any NFT launches with clear, concise, and consistent messaging that warns users of the dangers of phishing and offers tips to avoid falling for scams.

DDoS Attacks

NFTs can potentially be used to effectuate large-scale distributed denial-of-service (DDoS) attacks. This can occur where a malicious actor mints an NFT that points to a URL and airdrops* the NFT to thousands or even millions of users. Once deployed, all cryptocurrency wallets in receipt of the airdropped asset that are opened will load the NFT and direct traffic to the same URL, potentially resulting in a debilitating DDoS attack that could take down the website to which the URL points. All of this can be done without awareness by any of the NFT holders.

As cryptocurrencies, NFTs, and blockchain technology develop, continued education and information about the potential exploitation of new technology or digital assets remains critical for stakeholders and industry participants. For example, digital asset wallet providers and peer-to-peer exchanges will want to address all security vulnerabilities that could result in injury to their users or third parties.

IP Address Harvesting

By embedding custom code into NFTs, hackers can harvest IP addresses of individuals who view the NFTs on the web. Digital platforms that allow for peer-to-peer (P2P) exchange of NFTs may load this custom code when it is embedded in NFTs featured on their sites. Once an NFT-viewer's IP address is harvested, the developer who planted the code might be able to

identify the individual's geographic location (at least as detailed as the city). In addition, the developer might have access to the individual's real name and physical address if the IP address has been associated with such personal information elsewhere, such as on the dark web.

Further, the identification of an NFT-holder's geographic location can lead to kidnapping, not a remote fear in the cryptocurrency world, where industry participants can be worth millions of dollars.

Peer-to-peer marketplaces may need to consider how to prevent malicious HTML scripts from automatically loading on their sites and to disclose this risk to users. In addition, users can engage in good online hygiene by using a VPN, ensuring their passwords are secure, and updating them across all websites in order to avoid having their IP address associated with identifying personal information.

Platform Hacks

Platform vulnerabilities and exploits can cause significant financial loss to platform users. A recent example of this occurred when a large global NFT platform unwittingly facilitated sales of "inactive" NFT listings to savvy buyers who realized that sophisticated NFT-holders frequently transfer blue-chip NFTs to other wallets they control instead of de-listing them (which would require manual cancellation for a fee). By transferring the NFT between wallets, the NFT-holders were able to remove the public listing and avoid the fee associated with its cancellation. However, this process merely updated the listing from "active" to "inactive," allowing knowledgeable buyers to purchase the inactive NFTs via the smart contract instead of the exchange platform's user interface. While this particular exploit was addressed by the exchange platform after the fact, NFT industry participants should take care to plan and design products and user interfaces to protect users from inadvertent risk exposure.

NFT Media File Risks

When you buy an NFT, you typically are buying a token that points to a URL hosting a media file that is vulnerable to hacking, deprecation, or deletion. Any of these circumstances can result in the removal of the underlying media file, rendering the NFT worthless. To date, various approaches have been taken to protect NFT media files from security threats, including the use of decentralized databases such as the InterPlanetary File System (IPFS). NFT purchasers should remain aware of the security risks associated with NFT purchases and participate in the ecosystem with knowledge of the technology's limitations.

* Airdrop is a method of passive token distribution to cryptocurrency public keys.

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 multidisciplinary team of highly regarded attorneys advising clients on all things related to data and technology. 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

BakerHostetler

bakerlaw.com