ALERT MEMORANDUM

2024 Cybersecurity Developments: A Year in Review

January 31, 2025

The year 2024 saw cybersecurity and data privacy issues firmly remain at the forefront of corporate, governmental, and individual concerns. High-profile data breaches, including the largest theft of medical data in U.S. history, exposed the vulnerabilities of even well-established organizations, while federal and state regulators intensified their scrutiny of cybersecurity practices and disclosures. Legislative and regulatory efforts at both the state and federal levels continued to evolve, introducing stricter rules for data protection and incident reporting. Against this backdrop, enforcement actions and litigation underscored the rising costs of data breaches and the critical importance of proactive cybersecurity measures.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors.

NEW YORK

Jonathan Kolodner
+1 212 225 2690
jkolodner@cgsh.com

Rahul Mukhi
+1 212 225 2912
rmukhi@cgsh.com

Jenny Kline
+1 212 225 2832
jkline@cgsh.com

Michael Kowiak
+1 212 225 2929
mkowiak@cgsh.com

Data Breaches

2024 witnessed several high-profile cybersecurity breaches, illustrating the growing sophistication of cybercriminals despite increased determination by governments and private actors to prevent such attacks:

— In February, Change Healthcare, one of the biggest processors of patient billing in the country, announced that it had been hit by a ransomware attack. Beyond the disruption to the company and its clients, hackers allegedly also stole patients' health insurance information, medical treatment information, financial information, and government-issued identification numbers. The largest known theft of medical data in U.S. history, the breach reportedly impacted approximately 190 million people in the U.S.—over half of the country's population. Although the company reportedly paid a $22 million ransom to the hacker group known as BlackCat in an effort to keep data from being released, BlackCat's leadership allegedly appropriated the ransom and disappeared without paying the BlackCat affiliate responsible for the breach (the U.S. government offered a $10 million reward to anyone who could identify or locate key leadership in the hacking group). Because the aggrieved affiliate still had the compromised data, the affiliate then apparently attempted to extort a second ransom from the company. The chief executive of UnitedHealth Group was called to testify before the Senate Finance Committee in May to discuss the attack, and in December, the Nebraska AG filed a lawsuit against the company accusing it of security failings.

— In February, Cencora, a pharmaceutical company formerly known as AmerisourceBergen, experienced a ransomware attack that compromised patient data, including medical diagnosis and medication information. The company had reportedly obtained this patient data through its partnerships with drug makers in patient support programs, and at least 27 other pharmaceutical and biotechnology companies were affected in the cyberattack. While Cencora has yet to disclose details concerning how the attack was perpetrated or how many people in total were affected (at least 1.42 million individuals have been notified), this breach stands out because the company reportedly paid the hacking group Dark Angels $75 million over three Bitcoin transactions, the largest known cyber extortion payment to date. The payment, uncovered through analysis of unusual Bitcoin transactions, highlighted the financial toll of ransomware attacks and the vulnerabilities of data-sharing programs in the pharmaceutical sector and in other industries.

— In May, Snowflake Inc., a cloud provider, announced that it had suffered a data breach after threat actors exploited compromised login credentials to access customer accounts lacking multi-factor authentication. The attackers reportedly exfiltrated over 30 million bank account details, 28 million credit card numbers, and other customer and employee data from up to 165 of Snowflake's client accounts. In one instance, a major telecommunications company allegedly had around 50 billion customer call and text records compromised in Snowflake's breach. In October, a federal grand jury in Washington indicted two suspected hackers of Snowflake and charged them with 20 counts of conspiracy, computer fraud and abuse, extortion, wire fraud, and aggravated identity theft.

While these breaches are just a snapshot of the cybersecurity incidents in 2024, they reveal notable trends: (i) the total value of ransom payouts and the cost of addressing breaches continue to rise, (ii) governments are intensifying efforts to hold both bad actors and negligent companies accountable, and (iii) hacking groups are often unreliable, and fail to honor ransom agreements or maintain the confidentiality of payments.

Enforcement

In 2024, federal agencies continued to expand their oversight and enforcement of cybersecurity practices by targeting companies that failed to meet disclosure obligations, safeguard sensitive data, and implement adequate controls.

Securities and Exchange Commission (SEC)

— In June, the SEC settled an enforcement action against R.R. Donnelley & Sons Company (RRD), imposing a $2.125 million fine for alleged disclosure and internal control failures related to cybersecurity incidents that occurred in 2021. The SEC alleged that RRD: (i) lacked effective disclosure controls to ensure that important cybersecurity information was communicated to the appropriate management team responsible for making disclosure decisions, and (ii) failed to maintain adequate internal controls to restrict access to its IT systems and networks.

— In July, the U.S. District Court for the Southern District of New York dismissed key portions of the SEC's lawsuit against SolarWinds Corp. and its Chief Information Security Officer (CISO). The court rejected the SEC's claims of securities fraud and inadequate internal accounting controls related to the 2020 Sunburst cyberattack, ruling that cybersecurity controls do not fall within the SEC's jurisdiction over accounting controls. However, the court allowed the SEC to proceed with claims regarding allegedly misleading statements made by SolarWinds and its CISO about the company's cybersecurity posture, particularly those in the "Security Statement" on the company's website.

— In October, the SEC reached settlements with Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd., and Mimecast Limited for misleading disclosures regarding cybersecurity risks and the SolarWinds-related hacks that they experienced. Civil penalties ranged from $990,000 to $4 million, with Unisys paying the highest fine for allegedly portraying its cybersecurity risks as hypothetical despite known data exfiltration. Avaya was penalized for downplaying the scope of unauthorized file access. Check Point and Mimecast also faced fines for allegedly materially misleading disclosures about their cybersecurity incidents.

— In December, Flagstar Bancorp agreed to a $3.55 million settlement for making misleading statements about a 2021 cybersecurity attack that affected approximately 1.5 million people. The SEC alleged that the company understated the scope of the breach in its disclosures and failed to adequately report the incident, misleading investors by stating only that it had "in the past and may in the future be subject to cybersecurity attacks."

Department of Justice (DOJ)

— In May, the DOJ settled a False Claims Act (FCA) case with Insight Global LLC for $2.7 million based on alleged data security failures. The DOJ alleged that the company failed to safeguard personal health information during a COVID-19 contact tracing program for the Pennsylvania Department of Health by transmitting unencrypted emails, using shared passwords, and storing sensitive data in unsecured files, thereby violating its contractual data security obligations.

— In October, the DOJ settled an FCA case with ASRC Federal Data Solutions LLC (AFDS) after the company agreed to pay a $306,722 penalty and waived $877,578 in breach remediation costs. The settlement resolved allegations that AFDS and a subcontractor stored screenshots containing personal health information (PHI) on the subcontractor's server without individually encrypting the files.

Federal Trade Commission (FTC)

— In February, the FTC filed a complaint and proposed a consent order against Blackbaud, Inc., for misleading statements and unfair practices regarding its data retention related to a 2020 ransomware attack. In its complaint, the FTC asserted, for the first time, that a company can

engage in unfair practices by: (i) retaining data for longer than necessary, or (ii) failing to accurately communicate the severity and scope of a breach. Under the terms of the settlement, Blackbaud agreed to implement a comprehensive data security program, delete unnecessary backup files, and report future breaches to the FTC. The FTC case followed a separate $3 million SEC settlement in March 2023, in which Blackbaud was penalized for alleged inadequate disclosures regarding the same breach.

— In December 2024, the FTC announced a proposed settlement with Mobilewalla, Inc. that prohibited the company from selling sensitive location data, including information related to visits to health clinics, religious organizations, and political gatherings. The FTC alleged that Mobilewalla collected and sold this data without taking reasonable steps to verify consumers' consent, marking the first time the agency has labeled such practices as unfair. The proposed order also bans Mobilewalla from collecting consumer data from online real-time bidding advertising exchanges for purposes other than participating in those auctions.

New U.S. Legislation and Regulations

Pennsylvania's Breach of Personal Information Notification Act (BPINA)

Legislators were also busy in 2024. On July 28, 2024, Pennsylvania Governor Josh Shapiro signed amendments to BPINA which went into effect on September 26, 2024. Key changes include:

— *Attorney General Notification*. Entities notifying more than 500 PA residents must now also notify the Attorney General. The notification must include a summary of the breach, the date of the incident, and the total number of affected individuals.

— *Credit Monitoring and Reporting*. Breaches involving Social Security numbers, driver's license numbers, or bank account numbers require entities to offer 12 months of free credit monitoring and assume costs for one free credit report if individuals are otherwise ineligible for a free report.

— *Scope Adjustments*. Medical information notifications now apply only to state agencies or their contractors, which narrows the scope from the 2023 amendments.

— *Consumer Reporting Agencies Notification*. The threshold for notifying consumer reporting agencies was lowered from 1,000 to 500 individuals.

Utah's Online Data Security and Privacy Amendments

On March 19, 2024, Governor Spencer J. Cox signed Senate Bill 98, which, in part, amended the Protection of Personal Information Act and went into effect May 1, 2024. The amendments include:

— *Confidentiality Designation*. Information submitted to the Utah Attorney General or the Utah Cyber Center as part of a breach notification may be classified as confidential and protected, provided specific conditions are met. Similarly, information produced by the AG or the Center in providing coordination or assistance may also be deemed confidential.

— *Specific Notification Content*. Entities notifying the Attorney General and Utah Cyber Center must now include specific details, such as: (i) the date the breach occurred, (ii) the date the breach was discovered, (iii) the total number of people affected, including the number of Utah residents, (iv) the type of personal information involved, and (v) a brief description of the breach.

State Data Privacy Statutes

In 2024, seven states passed comprehensive data privacy statutes, and four states had state privacy laws that went into effect. Further, California and Colorado updated their existing data privacy legislation.

— *Enacted Statutes*. States that enacted data privacy statutes in 2024 include Kentucky, Maryland, Minnesota, Nebraska, New Hampshire, New Jersey, and Rhode Island.

— *Enforced Statutes*. States that began enforcing data privacy statutes in 2024 include Florida, Montana, Oregon, and Texas.

— *California*. New amendments to the California Consumer Privacy Act, enacted in September 2024, expanded the definition of "sensitive personal information" to include "neural data." Separately, the California Privacy Protection Agency proposed regulations requiring certain businesses to conduct annual cybersecurity audits. These regulations are still undergoing the formal rulemaking process and have not yet taken effect.

— *Colorado*. In May 2024, Colorado expanded the Colorado Privacy Act with amendments that will take effect on July 1, 2025. These changes include additional protections for biometric data that require entities to implement written retention and breach policies, obtain explicit consent, and limit the collection of biometric identifiers to specific purposes. Additional amendments enhance protections for minors' data when there is a heightened risk of harm.

State AI Statutes

While the United States currently lacks a comprehensive federal law regulating the development or deployment of artificial intelligence ("AI"), the 2024 legislative session saw significant activity at the state level. At least 45 states, along with Puerto Rico, the Virgin Islands, and the District of Columbia, introduced AI-related bills, and 31 states, Puerto Rico, and the Virgin Islands adopted resolutions or enacted legislation to address AI governance.

— *Utah*. In March 2024, Utah enacted the Utah Artificial Intelligence Policy Act, which went into effect in May 2024. The law imposes disclosure requirements on entities using generative AI tools to engage with their customers and limits the ability of those entities to attribute consumer protection violations to generative AI.

— *Colorado*. In May 2024, Colorado enacted comprehensive AI legislation that is set to take effect on February 1, 2026. The law requires developers and deployers of high-risk AI systems to exercise reasonable care to prevent algorithmic discrimination and mandates clear disclosures to consumers regarding the use of such systems.

— *New Hampshire*. In July 2024, New Hampshire enacted a law establishing the crime of fraudulent deepfake use, which went into effect on January 1, 2025. The law makes it a class B felony to knowingly create, distribute, or present a deepfake of an identifiable individual for purposes such as harassment, extortion, or reputational harm, and it provides a private cause of action for affected individuals.

Federal Regulations

Although the federal government has yet to pass a comprehensive cybersecurity statute, federal agencies have continued to promulgate and enforce rules around the prevention and reporting of data breaches.

— *SEC's Form 8-K Cybersecurity Guidance*. Throughout the spring of 2024, the SEC issued clarifying guidance on cybersecurity disclosures under Form 8-K. In May, the SEC clarified that, to avoid investor confusion, only material cybersecurity incidents should be disclosed under Item 1.05 of Form 8-K, while immaterial incidents may be voluntarily disclosed under Item 8.01. In June, the SEC further explained that disclosing information about material incidents to third parties, such as vendors or customers, is permissible, but such communications could trigger Regulation Fair Disclosure obligations if they involve selective disclosure of material nonpublic information.

— *SEC's Regulation S-P Updates*. In June 2024, the SEC finalized amendments to Regulation S-P that went into effect in August. The amendments enhance privacy and security requirements for broker-dealers, investment companies, registered investment advisers, and transfer agents. They also require covered institutions to implement incident response programs with written policies designed to detect, respond to, and recover from unauthorized access to customer information.

Additionally, institutions must now notify affected individuals within 30 days of discovering unauthorized access or use of sensitive customer information. If the institution cannot identify which specific individuals' information was impacted, the entity must notify everyone whose information was stored on the affected system. This notice obligation applies to any data elements that create a likely risk of fraud or identity theft, including partial Social Security numbers and other "authenticating information."

— *FTC's Health Breach Notification Rule*. In April 2024, the FTC finalized updates to its Health Breach Notification Rule that went into effect in May. The revised rule explicitly extends its applicability to health applications and similar technologies that handle identifiable health information. It also broadens the definition of a "breach of security" to include unauthorized disclosures, in addition to traditional data breaches. Covered entities must now provide detailed notifications to affected individuals, including information about third parties that acquired unsecured data, and may use electronic notifications. For breaches involving 500 or more individuals, entities are required to notify the FTC concurrently with affected individuals within 60 days of breach discovery.

— *FTC's Safeguards Rule Amendments*. In May 2024, amendments to the Gramm-Leach-Bliley Act's Safeguards Rule went into effect that introduced a new notification requirement for nonbank financial institutions. Institutions must now report breaches affecting 500 or more consumers via an online form on the FTC's website as soon as possible, but no later than 30 days after the discovery of the breach. The rule significantly broadens reporting obligations compared to state laws by: (i) covering all nonpublic, personally identifiable financial information, including basic details like names, (ii) requiring notification for any unauthorized sharing of customer information, even if intentional or voluntary, and (iii) mandating disclosure for all "notification events" involving 500 or more individuals, regardless of the risk of harm.

— *FCC Data Breach Notification Rule Updates.* In February 2024, the Federal Communications Commission (FCC) finalized modifications to its data breach notification rules that went into effect in March. The rules apply to telecommunications service providers, Voice over Internet Protocol providers, and telecommunications relay services providers. Key updates include an expanded definition of "breach" to cover inadvertent disclosures of PII and broader notification requirements for incidents involving any information that might identify a customer. Providers must report breaches affecting 500 or more customers within seven business days of determining a breach has occurred, while smaller breaches can be reported annually. However, the FCC no longer requires entities to notify customers if they can determine that no harm is likely to occur to the customer. The FCC also eliminated the mandatory seven-day waiting period before notifying customers, instead requiring notification "without unreasonable delay" and no later than 30 days after discovery.

— *CISA Proposed Rules under CIRCIA*. In April 2024, the Cybersecurity and Infrastructure Security Agency (CISA) published a Notice of Proposed Rulemaking to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Final rules are expected in late 2025. The proposed rules would require covered entities within critical infrastructure sectors to report: (i) covered cyber incidents within 72 hours, (ii) ransom payments within 24 hours, and (iii) substantial updates to previously submitted reports. Covered entities include those in critical sectors defined by Presidential Policy Directive 21, such as food and agriculture, real estate, and IT, though small businesses are exempt. Reportable incidents are limited to "substantial cyber incidents," including those causing significant loss of confidentiality, integrity, or availability, operational disruption, or

unauthorized access through third-party or supply chain compromises.

Litigation Developments

In 2024, courts continued to handle a significant volume of civil litigation related to cyberattacks and data breaches. As in past years, individuals whose PII was allegedly impacted in cyberattacks have continued to bring cases alleging statutory violations, negligence, unjust enrichment, breach of implied contract, and other related claims against victim company defendants.

While presiding over these matters, federal courts issued noteworthy decisions in 2024 related to questions of standing, immunity from civil litigation for certain entities under federal statute 42 U.S.C. § 233, and discovery.

Data Breach Standing Decisions

In 2024, many of the cyber-related decisions in federal court considered motions to dismiss on Fed. R. Civ. P. 12(b)(1) grounds, for lack of Article III standing. Defendants often argued that the primary alleged injury of increased risk of future identity theft following the cyberattack did not constitute an injury-in-fact. The decisions from the last year showed the fact-specific nature of the analysis on this issue and the different approaches taken across the circuits.

Data Breach Standing Decisions – No Standing Found

In *Greenstein v. Noblr Reciprocal Exchange*, the Ninth Circuit considered whether three plaintiffs had standing to bring a putative class action following a cyberattack that compromised certain driver's license numbers stored by the defendant insurance company.[1] The circuit court affirmed the district court's dismissal of the case on standing grounds.

The Ninth Circuit explained that two named plaintiffs' efforts to establish standing due to "an increased risk of future identity theft stemming from the cyberattack" failed in this case, because they did "not adequately allege[] their driver's license numbers were among those stolen in the attack."[2] Instead, the plaintiffs based their complaint on the incident notice they had received from the defendant, which said only that the recipient's driver's license data "*may* have been accessed."[3] Thus, the court characterized the named plaintiffs' claims that their driver's license numbers were stolen as "conclusory and unsupported."[4]

The Ninth Circuit also declined to find standing under the federal Drivers Privacy Protection Act, which restricts access to motor vehicle records. The circuit court held that although Congress can "elevat[e] to the status of legally cognizable injuries concrete *de facto* injuries that were previously inadequate in law," there must be a "close historical or common-law analogue for their asserted injury," which exposure of driver's license numbers lacked.[5]

The *Greenstein* decision was not the only case to find a lack of standing in the cyberattack context. For example, in *Burger v. Healthcare Management Solutions, LLC*, a district court in Maryland granted a motion to dismiss on standing grounds.[6]

The *Burger* litigation arose out of a ransomware attack against a subcontractor that assisted the federal government with Medicare administration, and that handled PHI and PII in connection with that role. The plaintiff had filed a putative class action against the subcontractor and a related contractor, alleging lack of adequate security procedures and inadequate protection of sensitive data.

The district court found that the plaintiff in *Burger* lacked standing due to a lack of injury-in-fact. In this respect, the district court noted that although the named plaintiff claimed she experienced unauthorized charges to her credit card following the cyberattack on the defendant, she "has not alleged that she had to pay

[1] 2024 WL 3886977 (9th Cir. Aug. 21, 2024).
[2] *Id.* at *1.
[3] *Id.* at *2.
[4] *Id.* at *2.
[5] *Id.* at *3.
[6] 2024 WL 473735 (D. Md. Feb. 7, 2024).

for any of the unauthorized charges, thereby undercutting any possible injury to her."[7]

Further, the *Burger* court held that the named plaintiff did not have standing due to a lack of traceability of any potential injury to the defendants. To this end, the court noted that although the plaintiff claimed she suffered fraudulent *credit card* charges, the breach only exposed her *bank account* information. Another alleged injury—of increased spam emails and calls—failed because the plaintiff did not allege her email address was exposed in the breach, again undercutting traceability.

These and the other claimed injuries did not satisfy the Fourth Circuit's standing requirements.[8] In any event, the district court found that the plaintiff's claims also warranted dismissal for failure to state a claim on which relief could be granted under Rule 12(b)(6).

Likewise, the district court in *In re Retreat Behavioral Health LLC* found a lack of standing in a case following a ransomware attack where unauthorized users gained access to the defendant's network and "may have accessed a data set" containing PHI/PII.[9]

The *Retreat* court noted that in the Third Circuit "disclosure of personal information does not amount to injury-in-fact where there are no specific allegations that a plaintiff's personal information has been used in a way that caused harm or that such use is certainly impending."

Because the "forensic investigation performed by Defendants merely revealed that an unauthorized person *may* have accessed a data set including Plaintiffs personal information" and there was no allegation "that [Plaintiffs'] PII and PHI data has been published or misused in any fashion" the district court concluded that any "allegations of hypothetical and future harm are too attenuated" for standing. The *Retreat* court distinguished this case from a prior Third Circuit decision finding standing where hackers posted plaintiff's personal information on the dark web.[10]

Data Breach Standing Decisions – Standing Found

Other federal court decisions in 2024 did find that plaintiffs whose PII was compromised had standing to bring cyberattack litigation against the entity that had stored their information. In those decisions, the district courts often proceeded to also hold that some but not all of the claims survived the defendants' efforts to dismiss on Rule 12(b)(6) grounds.

For example, in *In re Unite Here Data Security Incident Litigation*, a district court in New York held that plaintiffs had standing to bring claims related to a data breach of a labor union.[11] The district court noted that in the Second Circuit, "'plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data,' even where no such misuse of the data has yet occurred," based on a three-factor analysis (*i.e.* the *McMorris*[12] factors).

The *Unite Here* decision cited the alleged fact that cybercriminals perpetrated this data breach and that highly sensitive information such as Social Security numbers and health care information were compromised to conclude that an increased risk of identity theft constituting an injury-in-fact existed.

The district court reached this conclusion even though plaintiffs had not demonstrated that the second factor of the *McMorris* analysis—whether misuse of any of the data has occurred—weighed in favor of finding standing. The court noted that not all three factors of the *McMorris* analysis needed to point in favor of an injury-in-fact existing for standing to be found.[13]

[7] *Id.* at *6.
[8] In the context of identity theft (such as data breaches), the Fourth Circuit recognizes injury for purposes of standing "(1) through actual injury of identity theft; or (2) a threatened injury based on substantial risk of future identity theft that is sufficiently imminent." *Id.* at *5.
[9] 2024 WL 1016368 (E.D. Pa. Mar. 7, 2024).
[10] *Id.* at *2.
[11] 2024 WL 3413942 (S.D.N.Y. July 15, 2024).
[12] *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021).
[13] *But see De Medicis v. Ally Bank*, 2024 WL 1257022 (S.D.N.Y. Mar. 25, 2024) (another decision from 2024 applying the *McMorris* factors but finding that standing did not exist, including because the compromise of information

The *Unite Here* court also found traceability and redressability were satisfied for standing purposes. The court held that as to traceability "the complaint plausibly alleges that plaintiffs were subject to an increased risk of identity theft because important and sensitive information was stolen in the breach" and that "[t]raceability is a lower bar than proving causation on the merits."[14] The court then considered the motion to dismiss on Rule 12(b)(6) grounds, and denied the motion on all counts other than as to a New York statutory claim.

In *Keown v. International Association of Sheet Metal Air Rail Transportation Workers*, another district court found that standing existed.[15] In *Keown*, plaintiffs brought a putative class action regarding the alleged compromise of their PII in connection with a cyberattack on the national union to which they had previously belonged.

The *Keown* court noted that in the D.C. Circuit, standing is sufficiently pled if the plaintiff "plausibly alleges that the plaintiffs now face a substantial risk of identity theft as a result of [the defendant's] alleged negligence in the data breach," although a claim for damages must also allege another injury such as spending money or time on mitigation efforts.[16]

Applying this standard, the court held that both named plaintiffs had suffered an injury-in-fact for standing purposes. This was true both for the named plaintiff who alleged that his information had been posted on the dark web *and* for the plaintiff whose main alleged injury was increased threat of identity theft plus related harms. The court held that this sufficed to constitute injury-in-fact, including for damages, because the "increased risk" injury was coupled with the plaintiff's pursuit of mitigation measures.

However, the court dismissed the unjust enrichment claims and state statutory claims, as well as one of the two named plaintiffs' negligence claims under Rule 12(b)(6), so that only the implied breach of contract claim and one plaintiff's negligence claim remained.[17]

42 U.S.C. § 233

In *Ford v. Sandhills Medical Foundation, Inc.*, the Fourth Circuit considered if a "nonprofit health center that receives federal funding" was immune from a civil suit following a cyberattack that it suffered, which allegedly exposed the PII of the individual plaintiffs.[18]

This case arose against the backdrop of a federal statute that provides immunity to private health centers that receive federal funding from damages "resulting from the performance of medical, surgical, dental, or related functions."[19] In *Ford*, the appellate court was required to resolve whether the data breach compromising PII that the health center experienced constituted a "related function[]" under the statute, in which case the health center was immune from suit and the United States would be substituted in as the defendant.

The Fourth Circuit concluded that Section 233 did not provide immunity to the health center for the data breach that compromised patient PII, including because "the storage of patient PII" was not a "medical, surgical, dental, or related function" based on the language of the statute. As a result, the health center remained the defendant in the litigation that

was connected to "an inadvertent programming error and not any targeted attempt" to acquire the information).

[14] *Unite Here*, 2024 WL 3413942, at *4.

[15] 2024 WL 4239936 (D.D.C. Sept. 19, 2024).

[16] *Id.* at *3.

[17] *See also Briggs v. North Highland Co.*, 2024 WL 519722 (N.D. Ga. Feb. 9, 2024) (finding that "the hack and the nature of the information alleged to have been stolen . . . raises a substantial risk of identity theft" and suffices for standing in seeking injunctive relief, and that when coupled with claim of emotional distress, plaintiff had also alleged injury-in-fact for purposes of seeking damages); *In re Sequoia Benefits and Insurance Data Breach Litigation*, 2024 WL 1091195 (N.D. Cal. Feb. 22, 2024) (denying motion to dismiss on Rule 12(b)(1) grounds including because plaintiffs pled there was "material risk of fraud and identity theft caused by the data breach" and because plaintiffs spent "significant time monitoring their accounts to check for identity theft" which constituted injury-in-fact for damages claim).

[18] 97 F.4th 252 (4th Cir. 2024).

[19] 42 U.S.C. § 233.

challenged its security practices. A petition for certiorari has subsequently been filed.

Discovery Related Decisions

A Special Master appointed by the District Court for the District of New Jersey considered whether materials that a cybersecurity firm—Stroz Friedberg ("Stroz")—prepared in connection with its analysis of a data breach that impacted its client were privileged.[20]

The Special Master concluded that a slide deck and incident analysis that Stroz had prepared regarding the breach were not privileged and had to be produced in related civil litigation. In reaching this conclusion, the Special Master emphasized that although the client's counsel had engaged Stroz, Stroz circulated its findings to both counsel and the client, which undermined the argument that Stroz's work was only to benefit the law firm in providing legal advice.[21]

However, the Special Master concluded that a memorandum that Stroz drafted about the incident and provided only to counsel *was* subject to privilege and protected from production, because its purpose was to facilitate the provision of legal advice to the client rather than for its business purposes.[22]

Key Takeaways

Data Breaches – Malware and ransomware attacks continue to rise in frequency and sophistication, targeting cloud-based systems and exploiting vulnerabilities to exfiltrate vast amounts of sensitive data, including financial records and health information.

Enforcement Actions – The SEC, DOJ, and FTC were all active enforcers in 2024, which underscores the agencies' increasing focus on accountability for both the prevention of cyber incidents and the transparency and accuracy of public disclosures when breaches occur. Of course, with the new Trump Administration, it remains to be seen whether, and to what extent, these will remain a focus given the Administration's priorities.

Legislation and Regulations – Lawmakers and regulatory agencies across the U.S. made significant strides in addressing cybersecurity and data privacy concerns in 2024 as efforts to pass a federal statute continued to stall. States enacted and updated breach notification and privacy laws, while federal agencies introduced new rules to enhance data protection and incident responses. These efforts reflect an ongoing trend toward stricter regulatory oversight and increased accountability for protecting sensitive information. Again, it will be important to closely monitor the new Trump Administration and Congress to understand whether, at the federal level, there are changes to the approach of the last four years.

Civil Litigation – There is no sign that litigation against entities that suffer cyberattacks or data breaches—for their alleged failure to adequately protect plaintiffs' PII/PHI—will slow in the near future. Because courts continue to engage in highly fact-specific analysis regarding Article III standing, seeking to dismiss for lack of standing remains a common if only sometimes successful strategy, in tandem to seeking dismissal on Rule 12(b)(6) grounds.

…

CLEARY GOTTLIEB

[20] *Customer Data Security Breach Litigation*, 2024 WL 3861330 (D. N.J. Aug. 19, 2024).

[21] *Id.* at *14.

[22] *Id.* at *16.