CLEARY GOTTLIEB

2021 Cybersecurity and Privacy Developments in the United States

January 2022

Overview

As reflected in a recent survey of chief legal officers, cybersecurity has overtaken compliance as the most significant legal risk that businesses face today.[1] More than 50% of executives expect a surge in reportable cyber incidents in 2022 as compared to 2021, according to another recent survey.[2] This should come as no surprise, as last year brought a series of high-profile cyberattacks on major companies and U.S. infrastructure targets, continuing the trend seen in recent years. Regulators also brought a number of cybersecurity enforcement actions and announced new rules, guidance, and initiatives on ransomware and other cyber-related issues. In addition, after many years of debate, Congress made some progress in crafting legislation that would require certain companies to report significant cyberattacks and ransomware payments to the U.S. federal government. Companies should expect the demands of cybersecurity risk management and oversight to intensify as we enter 2022.

In this publication, we highlight some of the most significant cybersecurity and privacy developments of 2021 in the United States and predict key challenges and areas of focus for the coming year. A subsequent publication will address developments in the European Union and in other jurisdictions outside the United States.

[1] Ass'n of Corp. Counsel, *2021 ACC Chief Legal Officers Survey* (Mar. 2021), https://www.acc.com/clo2021.

[2] PricewaterhouseCoopers, *2022 Global Digital Trust Insights Survey* (Oct. 2021), https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html.

Data Breaches and Other Cyberattacks

2021 saw a number of high-profile data breaches, ransomware attacks, and other cyber incidents affecting both private sector businesses and public infrastructure, and further driving the conversation on cybersecurity risk:

— Colonial Pipeline, one of the largest fuel pipelines in the United States, suffered a ransomware attack that disrupted fuel supplies across the United States. The company paid $4.4 million in ransom, part of which was recovered by U.S. law enforcement.

— CNA Financial, a large commercial insurer, announced that it suffered a ransomware attack that caused the company to pay $40 million to regain access to its data.

— Cyber criminals demanded $50 million from computer manufacturer ACER after breaching the company's systems. The company refused to pay the ransom demand, which was subsequently raised to $100 million, and was targeted again in a cyberattack in October.

— One of the country's largest meat suppliers, JBS USA, disclosed a ransomware attack that temporarily halted operations and led to an $11 million ransom payment.

— An Iowa-based provider of agricultural services, NEW Cooperative, suffered a ransomware attack resulting in a $5.9 million ransom demand that would increase to $11.8 million if the ransom was not paid within a five-day period. The company refused payment.

— Microsoft announced that a Microsoft Exchange hack exposed vulnerabilities in its email software, affecting over 30,000 organizations across the United States.

— Airline technology provider SITA announced that it suffered a data breach affecting approximately 2 million airline passengers. The stolen information included program card numbers, status level information, and, in some cases, customer names.

U.S. Enforcement

In response to continuing significant data breaches and other cyber incidents, regulators were increasingly active in bringing cybersecurity enforcement actions against companies that allegedly maintained inadequate cybersecurity protections or that failed to comply with related disclosure obligations. This reflects a continuing trend in which companies victimized by attackers become the subjects of regulatory investigations:

— In March, the New York State Department of Financial Services (DFS) brought an enforcement action against Residential Mortgage Services, Inc. (RMS) for allegedly violating DFS's cybersecurity regulations requiring timely reporting of data breaches and comprehensive cybersecurity risk assessments. RMS, a licensed mortgage banker, collected sensitive personal data of mortgage loan applicants as part of its business operations. After a July 2020 examination, evidence was uncovered showing that RMS had failed to report a cybersecurity breach involving unauthorized access to the e-mail account of an RMS employee with access to a significant amount of that data. RMS agreed to pay a $1.5 million penalty.

— In June, the Securities and Exchange Commission (SEC) announced a settlement with First American Financial Corporation (First American) for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed customer information. After a journalist informed First American of a flaw in its systems, the company issued a public statement noting that it had shut down external access to the document-sharing application that had exposed customer information and that it had no preliminary indication of large-scale unauthorized access. However, at the time of this disclosure, senior management was unaware that the company's information security personnel had identified the vulnerability several months earlier and had failed to remediate it. Thus, the SEC charged the company with maintaining deficient disclosure controls and procedures, even absent a third-party breach or intrusion of the company's systems. As part of its settlement with the SEC, the company agreed to pay a $487,616 penalty.

— The SEC has also been conducting a sweep of public companies relating to the cyberattack involving software made by SolarWinds Corp., which became public in December 2020.[3] The SEC has sought information on a voluntary basis from companies that may have used the compromised versions of SolarWinds software, and it has advised companies that if they cooperate by providing the requested information and making any required disclosures, the SEC will not recommend an enforcement action against recipients of the request relating to disclosure controls and procedures. However, the SEC has also asked companies responding to the request to not only provide information about the impact of SolarWinds, but also to provide information about other cybersecurity incidents involving external attacks. The sweep demonstrates the aggressive approach that the SEC is taking to evaluating companies' responses to cyberattacks both from disclosure and disclosure controls perspectives.

[3] U.S. Sec. and Exch. Comm'n, *In the Matter of Certain Cybersecurity-Related Events* (HO-14225) FAQs, https://www.sec.gov/enforce/certain-cybersecurity-related-events-faqs.

Data Security and Privacy Rules, Guidance, and Initiatives

Separate from enforcement actions, U.S. regulators and agencies issued new rules, guidance, and initiatives on cyber-related topics, including ransomware and cyber-incident notification.

The Federal Trade Commission

— In April, the Federal Trade Commission (FTC) published a blog post emphasizing the need for companies to prioritize data security, including by ensuring that data security considerations are elevated to the C-Suite and Board level. The FTC laid out five recommendations for companies in this context: (1) make data security a priority, including by establishing Board-level oversight and engaging a broad range of company personnel beyond the IT department; (2) allocate necessary resources to understanding cybersecurity risks and challenges; (3) ensure that security programs are tailored to a company's unique needs and go beyond meeting baseline compliance obligations; (4) implement both a strong data security program and a robust incident response plan; and (5) learn from the experience of companies that have been impacted by data breaches and other cyber incidents.[4]

— In October, the FTC announced updates to the Safeguards Rule, which was mandated under the 1999 Gramm-Leach-Bliley Act and requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure. The FTC's October 2021 updates to the Rule include a requirement for non-banking financial institutions (such as mortgage brokers, motor vehicle dealers, and payday lenders) to develop, implement, and maintain a comprehensive system to secure their customers' data. The changes also include more specific criteria for the types of data security protections financial institutions must adopt as part of their information security programs, such as using encryption and limiting access to consumer data, as well as requirements for financial institutions to adequately explain their information sharing practices and to designate a single qualified individual to oversee their information security programs.[5]

— The FTC also issued a notice of proposed rulemaking seeking public comment on a proposal to further amend the Safeguards Rule. Under the proposal,

[4] For further information, see the Cleary Gottlieb publication "FTC to Corporate Boards: Mind Your Data Security" at https://www.clearycyberwatch.com/2021/04/ftc-to-corporate-boards-mind-your-data-security/.

[5] Press Release, "FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches," Fed. Trade Comm'n (Oct. 27, 2021), https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial.

financial institutions would be required to report any security event where misuse of customer information has occurred or is reasonably likely to occur and where at least 1,000 consumers have been or may reasonably be affected.[6]

The Department of the Treasury / OFAC

— In September, the Treasury Department's Office of Foreign Assets Control (OFAC) issued an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, which highlights the sanctions risks associated with making ransomware payments. The advisory stresses that the U.S. government "strongly discourages" making ransomware payments and instead "recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks."[7] Later, in October, OFAC issued Sanctions Compliance Guidance for the Virtual Currency Industry, which, among other things, provides information for companies in evaluating sanctions-related risks, building sanctions compliance programs, protecting their businesses from misuse of virtual currencies, and understanding OFAC's recordkeeping, reporting, licensing, and enforcement processes.

— Subsequently, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued an Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, which updates and replaces its previous advisory from 2020. The FinCEN Advisory examines the role of financial intermediaries in facilitating ransomware payments, which are generally paid using virtual currencies like Bitcoin; identifies trends, typologies, and financial red flags of ransomware and associated payments; and stresses the legal obligations of U.S. financial institutions in the ransomware context – for example, to report suspicious transactions that may involve ransom payments to criminal actors.[8]

The Department of Justice

— Given the proliferation of ransomware actors demanding ransom payments in the form of cryptocurrency, in October, the Department of Justice announced the creation of a National Cryptocurrency Enforcement Team (NCET) to oversee complex investigations and prosecutions of criminal misuses of cryptocurrency.[9] The NCET will draw upon DOJ's Cryptocurrency Enforcement Framework, released in October 2020.[10]

— The Department of Justice also announced the launch of a new Civil Cyber-Fraud Initiative, which will use the False Claims Act to pursue cybersecurity-related fraud committed by government contractors and grant recipients. The initiative is focused on pursuing companies that "knowingly provid[e] deficient cybersecurity products or services, knowingly misrepresent[] their cybersecurity practices or protocols, or knowingly violat[e] obligations to monitor and report cybersecurity incidents and breaches."[11]

---

[6] Fed. Trade Comm'n, *Standards for Safeguarding Customer Information*, 86 Fed. Reg. 70062 (Dec. 9, 2021).

[7] U.S. Dep't of the Treasury, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf. For further information, see the Cleary Gottlieb publication "OFAC Updates Ransomware Advisory and Sanctions Virtual Currency Exchange" at https://www.clearycyberwatch.com/2021/09/ofac-updates-ransomware-advisory-and-sanctions-virtual-currency-exchange/.

[8] For further information, see the Cleary Gottlieb publication "OFAC Ramps up Targeting of Ransomware-linked Actors and FinCEN Updates Ransomware Advisory" at https://www.clearycyberwatch.com/2021/11/ofac-ramps-up-targeting-of-ransomware-linked-actors-and-fincen-updates-ransomware-advisory/.

[9] Press Release, "Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team," U.S. Dep't of Justice (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

[10] U.S. Dep't of Justice, *Cryptocurrency Enforcement Framework* (Oct. 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.

[11] Press Release, "Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative," U.S. Dep't of Justice (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

Other Federal Regulators and Agencies

— In November, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency (OCC), and the Board of Governors of the Federal Reserve System announced a final rule requiring banking organizations to notify their primary regulator of certain significant computer-security incidents within 36 hours. The rule separately requires bank service providers to notify their bank customers if they experience a cyber-incident that causes a material disruption of services that lasts for four or more hours.[12]

— In December, the OCC issued its Semiannual Risk Perspective, which highlighted the operational risks that companies face from sophisticated cyber-attacks. The OCC issued several recommendations for banks, including that they should: (1) "adopt robust threat and vulnerability monitoring processes"; (2) "implement stringent and adaptive security measures"; (3) properly configure network systems and "have effective patch management processes in place"; (4) "ensure that critical systems and records are backed up and stored in immutable formats"; and (5) assess risks from third parties to develop "a comprehensive approach to operational resilience."[13]

— Also in December, federal agencies – including the Cybersecurity and Infrastructure Security Agency (CISA) – announced the discovery of a critical security flaw in the open-source, Java-based Log4j software that is embedded in countless commercial software platforms, websites, and digital applications. CISA released guidance for companies to remediate any associated vulnerabilities on their systems, and the FTC issued a clear warning that companies have a legal duty to mitigate known software vulnerabilities – including Log4j – that risk harm to consumers and may face legal action from the FTC if they fail to do so.[14]

New York State Department of Financial Services

— This past June, DFS issued new ransomware guidance, noting that "key cyber hygiene measures must be in place to mitigate the risk of a successful attack."[15] The guidance stressed that regulated companies should report any successful deployment of ransomware to DFS as promptly as possible and within 72 hours at the latest. DFS expects companies to take a multi-layered approach to cybersecurity, including by employing email filtering and anti-phishing training, vulnerability/patch management, multi-factor authentication, password management, privileged access management, and adequate monitoring and response protocols, along with adopting an incident response plan that explicitly addresses ransomware attacks.

[12] For further information, see the Cleary Gottlieb publication "Banking Regulators Approve Final Rule Establishing Cyber Incident Notification Requirements" at https://www.clearycyberwatch.com/2021/12/banking-regulators-approve-final-rule-establishing-cyber-incident-notification-requirements/.

[13] Office of the Comptroller of the Currency, National Risk Committee, *Semiannual Risk Perspective: Fall 2021* (Dec. 6, 2021), https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2021.pdf. For further information, see the Cleary Gottlieb publication "The Office of the Comptroller of the Currency Warns of Increasingly Complex Cyber Risks for Banks" at https://www.clearycyberwatch.com/2021/12/the-office-of-the-comptroller-of-the-currency-warns-of-increasingly-complex-cyber-risks-for-banks/.

[14] For further information, see the Cleary Gottlieb publication "The Federal Trade Commission Warns Companies to Remediate the 'Log4j' Software Security Vulnerability" at https://www.clearycyberwatch.com/2022/01/the-federal-trade-commission-warns-companies-to-remediate-the-log4j-software-security-vulnerability/.

[15] N.Y. Dep't of Fin. Servs., *Ransomware Guidance* (June 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.

U.S. Legislation and Executive Action

— *California*. After passing the California Privacy Rights Act (CPRA) in 2020 (which itself amended and expanded California's earlier Consumer Privacy Act), the California state legislature in 2021 expanded the definition of "personal information" under the state's breach notification law to include genetic data.[16] This in turn expanded the scope of personal information covered by the private right of action provided under the California Consumer Privacy Act (CCPA) and CPRA. The legislature also enacted the Genetic Information Privacy Act, which regulates direct-to-consumer genetic testing companies and associated vendors and requires such companies to obtain consumers' express consent for the collection, use, and disclosure of genetic data.[17]

— *Virginia*. In March 2021, Virginia became the second state in the nation after California to enact comprehensive data privacy legislation. The Virginia Consumer Data Protection Act (CDPA), which will take effect in 2023, applies to certain entities that: (i) conduct business in Virginia or that produce products or services that target Virginia residents; and (ii) meet one of two thresholds with respect to the number of Virginia consumers whose personal data the entity controls or processes. The Act provides various rights to Virginia consumers, including the rights to access, correct, and delete their personal information collected by covered entities and the right to opt-out of the processing or sale of their personal data by covered entities in certain circumstances. It also requires covered entities to, among other things, adopt data minimization and data security measures; disclose their privacy practices through a meaningful privacy notice; enter into data processing agreements and conduct data protection assessments before performing certain processing activities; and obtain affirmative consent prior to processing certain sensitive personal data.[18]

— *Colorado*. Subsequently, in July 2021, Colorado became the third state to enact comprehensive privacy legislation with the adoption of the Colorado Privacy Act (ColoPA). As with the CDPA in Virginia, the ColoPA draws heavily from California's privacy laws and the European Union's General Data Protection Regulation (GDPR). The ColoPA applies to certain entities that: (i) conduct business in

[16] Cal. Civ. Code §§ 1798.29, 1798.81.5 (2020), *amended by* A.B. No. 825 (2021).

[17] Cal. Civ. Code § 56.18 (2022).

[18] For further information, see the Cleary Gottlieb publication "The 'New' Dominion of Privacy Law: Virginia Becomes Second State to Pass Comprehensive Consumer Data Privacy Act" at https://www.clearygottlieb.com/-/media/files/alert-memos-2021/the-new-dominion-of-privacy-law-virginia-becomes-second-state.pdf.

Colorado or that produce products or services that intentionally target Colorado residents; and (ii) meet one of two thresholds with respect to the number of Colorado consumers whose personal data the entity controls or processes. Among other things, the ColoPA provides Colorado consumers the rights of access, correction, and deletion; imposes a variety of duties and obligations on covered entities, including the duties of transparency, data minimization, care, and obtaining affirmative consent before processing sensitive data; and requires entities to enter into data processing agreements and conduct data protection assessments before performing certain processing activities.[19]

— *Connecticut*. Connecticut enacted two new data privacy laws in 2021, which became effective this past October. The first law, Public Act No. 21-59, amended Connecticut's existing data breach notification law by expanding the definition of "personal information," reducing the maximum time for required notifications, and protecting from public disclosure certain information provided during an investigation following a data breach.[20] The second law, Public Act 21-119, shields companies from punitive damages in tort suits alleging that their failure to implement reasonable cybersecurity controls resulted in a data breach if those companies had in fact implemented a formal cybersecurity program that met industry standards.[21]

— *Texas*. The Texas state legislature expanded its notification requirements for companies suffering data breaches in a 2021 amendment to the Texas Identity Theft Enforcement and Protection Act.[22] Among the changes is a requirement that the Texas Attorney General post data breach notifications affecting Texas residents on a publicly accessible website.

— *Other States*. Several dozen other U.S. states enacted or introduced legislation in 2021 on cybersecurity issues. Many of the bills and resolutions set new cybersecurity standards for public agencies and private companies,[23] created new state agencies or empowered existing state agencies to deal with cybersecurity threats,[24] and/or commissioned studies on the effects of rising cybersecurity threats.[25]

— *Federal Legislation*. Although Congress did not pass comprehensive federal data security or privacy legislation in 2021, the number of proposals for legislation requiring stronger cybersecurity responses and mechanisms increased substantially. Bipartisan support exists for legislation requiring the reporting of certain cyber intrusions affecting federal agencies, government contractors, and critical infrastructure owners and operators to CISA, although differences about the mechanics of such a requirement are still being resolved. Other proposals include an amendment to the National Defense Authorization Act to provide CISA with rulemaking authority to set standards for cybersecurity protocols for federal agencies and contractors.

— *Cybersecurity Executive Order*. On May 12, 2021, President Biden signed an Executive Order on Improving the Nation's Cybersecurity (EO 14028). Among other things, EO 14028:

- requires federal information technology and operational technology contractors to share threat information with federal law enforcement agencies and cooperate in investigating potential cyber incidents;

[19] For further information, see the Cleary Gottlieb publication "The Centennial State Claims a New Number: Colorado to Become Third State in the U.S. to Enact Comprehensive 'Privacy Act'" at https://www.clearygottlieb.com/-/media/files/alert-memos-2021/the-centennial-state-claims-a-new-number.pdf.

[20] Conn. H.B 5310, Public Act No. 21-59 (2021).

[21] Conn. H.B. 6607, Public Act No. 21-119 (2021).

[22] Tex. Bus. & Com. Code § 521.053 (2009), *amended by* Tex. H.B. No. 3746 (2021).

[23] *See, e.g.*, Md. S.B. No. 49 (2021).

[24] *See, e.g.*, Iowa H.B. No. 861 (2021).

[25] *See, e.g.*, Va. H.J.R. No. 64 (2021); La. H.C.R. No. 108 (2021).

- requires federal agencies to prioritize the adoption of cloud technology using Zero Trust Architecture, which limits user access to an as-needed basis in attempt to minimize the risk of breaches, and to deploy multifactor authentication and encryption;
- establishes baseline security standards for software sold to the federal government;
- stands up a Cyber Safety Review Board, comprised of government and private sector representatives, to review significant cyber incidents and to share lessons learned;
- charges CISA with developing a standardized playbook and set of definitions for cyber vulnerability assessment and incident response by federal agencies;
- directs federal agencies to improve their endpoint detection-and-response (EDR) capabilities in order to better detect cybersecurity vulnerabilities and incidents on federal government networks; and
- charges the Department of Homeland Security with developing standardized requirements for maintaining information event logs for federal agencies.[26]

[26] Exec. Order No. 14028 (2021).

U.S. Litigation

There were also significant developments in cyber-related litigation in 2021:

— In January, a California federal judge granted a motion to dismiss filed by Marriott International, Inc. ("Marriott") in a class action related to a data breach, holding that the plaintiff lacked standing to sue.[27] The court agreed with Marriott that the information obtained in the data breach was not "sensitive" enough to establish an injury for federal standing purposes. The decision is one of several in 2021 that grappled with standing in data breach cases.

- For example, in February, the Eleventh Circuit dismissed claims brought in a putative class action seeking damages for disclosure of credit card information in a data breach of Captiva MVP Restaurant Partners, LLC. The court held that the plaintiff could not establish standing based on allegations that the breach created a "continuing increased risk of harm from identity theft and identity fraud" or that the plaintiff took affirmative steps to mitigate such potential harm.[28] In so doing, the Eleventh Circuit joined the Second, Third, Fourth, and Eighth Circuits in requiring allegations that an increased risk of identity theft due to a data breach is not merely hypothetical. By contrast, the Sixth, Seventh, Ninth, and D.C. Circuits generally confer standing on plaintiffs based merely on allegations of such an increased risk.

- In April, the Second Circuit affirmed the dismissal of a proposed class action against Carlos Lopez & Associates, LCC, regarding a mistaken disclosure of personal identifying information, due to lack of standing.[29] This case marked the first time the Second Circuit explicitly adopted the standard that plaintiffs may establish standing based on an "increased-risk" theory; however, the court held that plaintiff did not meet the standard in that particular case.

[27] For further information, see the Cleary Gottlieb publication "The Central District Court of California Grants Marriott International's Motion to Dismiss in Data Breach Suit" at https://www.clearycyberwatch.com/2021/01/the-central-district-court-of-california-grants-marriott-internationals-motion-to-dismiss-in-data-breach-suit/.

[28] For further information, see the Cleary Gottlieb publication "11th Circuit Rejects Standing Based on Heightened Risk of Identity Theft in Data Breach Suit" at https://www.clearycyberwatch.com/2021/03/11th-circuit-rejects-standing-based-on-heightened-risk-of-identity-theft-in-data-breach-suit/.

[29] For further information, see the Cleary Gottlieb publication "Second Circuit Articulates Injury Standard in Data Breach Suits" at https://www.clearycyberwatch.com/2021/05/second-circuit-articulates-injury-standard-in-data-breach-suit/.

- In June, in class action litigation against TransUnion stemming from alleged violations of the Fair Credit Reporting Act, the U.S. Supreme Court issued a decision limiting consumers' standing to sue if the alleged harm, such as from disclosure of misleading credit reports, does not actually materialize.[30] In its 5-4 ruling, the Court expressed serious doubts that the risk of future harm, standing alone, could be sufficient to demonstrate standing in any suit for damages. While it did not specifically relate to standing to sue in the data breach context, the Supreme Court's decision may call into question the approach of circuit courts that have allowed plaintiffs in data breach cases to establish standing based merely on an increased risk of identity theft or fraud. Indeed, the decision has potential implications for a wide variety of cyber-related cases where personal information may be exposed but not necessarily used for fraudulent activity.[31]

— California data breach law continues to develop in response to the CCPA's creation of a private right of action, with nearly 100 CCPA-related cases filed throughout 2021. Notably, in February, a federal judge in California dismissed a CCPA claim in a putative class action against Alphabet, Inc. and Google, LLC, after the plaintiff conceded that his allegations failed to state a claim under the statute. Specifically, the plaintiff alleged that the defendant companies failed to adequately disclose or obtain consent for their data collection practices. However, § 1798.150 of the CCPA confers a private right of action for claims related to "unauthorized access and exfiltration, theft, or disclosure as a result of [a] business's violation of the duty to implement and maintain reasonable security procedures and practices."[32] Since there were no allegations of a security breach in the case, the CCPA claim was dismissed.[33]

— In October, the Delaware Court of Chancery dismissed a shareholder derivative action concerning Marriott's discovery of a data breach for failure to make a pre-suit demand and failure to plead sufficient facts to establish demand futility.[34] The court found that the Marriott board members did not face a substantial likelihood of liability stemming from the breach, as they had not failed to undertake their oversight abilities, turned a blind eye to compliance violations, or consciously failed to remediate cybersecurity failures. Thus, the board retained its ability to assess whether to pursue litigation on behalf of the company and the derivative action was improper.

[30] *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).

[31] For further information, see the Cleary Gottlieb publication "Data Breach Class Action Against Bonobos Dismissed For Lack of Standing" at https://www.clearygottlieb.com/news-and-insights/publication-listing/data-breach-class-action-against-bonobos-dismissed-for-lack-of-standing.

[32] Cal. Civ. Code § 1798.150.

[33] *McCoy v. Alphabet, Inc.*, No. 20-CV-05427-SVK, 2021 WL 405816, at *8 (N.D. Cal. Feb. 2, 2021).

[34] *Firemen's Ret. Sys. of St. Louis ex rel. Marriott Int'l, Inc. v. Sorenson*, No. CV 2019-0965-LWW, 2021 WL 4593777 (Del. Ch. Oct. 5, 2021).

Key Takeaways

— Cybersecurity continues to be a critical risk for businesses of all types due to increased dependence on technology, a pandemic-generated shift to remote work arrangements, and the continued proliferation of data breaches, ransomware attacks, and other cyber intrusions.

— Ransomware in particular represents an increasing concern for companies from across industries, due to the substantial costs, legal risks, and reputational concerns.

— Given the continued proliferation of significant cyber incidents, and the recognized need to further incentivize cooperation between private entities and government agencies in preventing, investigating, and remediating cyberattacks, it is increasingly likely that Congress will enact federal data security legislation in some form in the coming year. Additionally, state legislatures are likely to continue to expand their data security and privacy laws, subjecting businesses to additional requirements and reporting obligations. Company management should continue to provide regular updates to their Boards and senior leadership on developments in the law to keep abreast of their companies' evolving obligations in this area.

— Increased regulatory action related to cybersecurity issues reflects the continued shift away from regulators viewing hacked companies as only victims and toward potentially holding them responsible for perceived deficiencies in their cybersecurity programs and other internal policies and procedures. Importantly, regulators like the SEC are focused on whether and how a company maintains disclosure controls and procedures to ensure that management is adequately and timely informed of cyber incidents that warrant public disclosures. We expect these trends to continue in 2022 as the Biden administration enters its second year.

— Private litigation arising out of data breaches continues to proliferate. In dismissing the shareholder derivative action following a data breach in the Marriott case, for example, the Delaware Court of Chancery nevertheless noted that "corporate governance must evolve to address" cybersecurity risks and that "[t]he corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place."[35]

— Collectively, these trends underscore the need for company management and directors to take an active role in establishing adequate cyber defenses and responses to incidents. This is especially true because we expect these trends to continue into 2022, both in the U.S. and globally, requiring companies to monitor the evolving legal landscape.

CLEARY GOTTLIEB

[35] *Marriott*, 2021 WL 4593777, at *12.

Contacts

Jonathan S. Kolodner
Partner
New York
+1 212 225 2690
jkolodner@cgsh.com

Aaron Francis
Associate
New York
+1 212 225 2277
aafrancis@cgsh.com

Daniel Ilan
Partner
New York
+1 212 225 2415
dilan@cgsh.com

Hyatt Mustefa
Associate
New York
+1 212 225 2628
hmustefa@cgsh.com

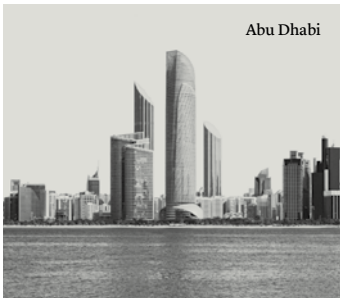
Rahul Mukhi
Partner
New York
+1 212 225 2912
rmukhi@cgsh.com

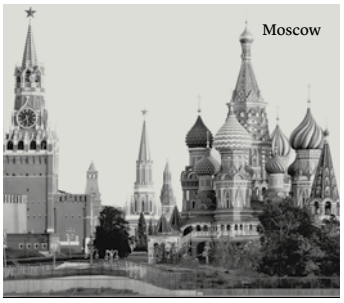
Lilianna (Anna) Rembar
Associate
New York
+1 212 225 2328
lrembar@cgsh.com

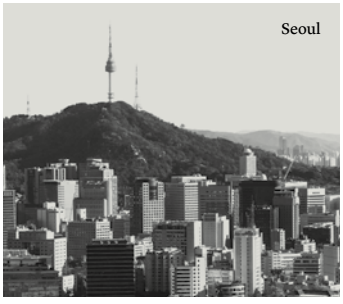
Anthony M. Shults
Senior Attorney
New York
+1 212 225 2693
ashults@cgsh.com

Melissa Faragasso
Associate
New York
+1 212 225 2115
mfaragasso@cgsh.com

CLEARY GOTTLIEB







clearygottlieb.com

220118.09_012722