COVID-19 considerations for SEC cybersecurity guidance, disclosure, enforcement, and parallel proceedings: navigating the new normal

Aldo M. Leiva and Michel E. Clark

Abstract

Purpose – *To examine the COVID-19 pandemic's effects on regulated entities within the context of cybersecurity, US Securities and Exchange Commission (SEC) compliance, and parallel proceedings.*

Design/methodology/approach – *Describes the SEC's ability to conduct its operations within the telework environment, its commitment and ability to monitor the securities market, its enhanced monitoring of the adverse effects of SEC-regulated companies from COVID-19, its guidance to public companies of disclosure obligations related to cybersecurity risks and incidents, the SEC Office of Compliance and Examinations's (OCIE's) focus on broker-dealers' and investment advisories' cybersecurity preparedness, the role and activities of the SEC Division of Enforcement's Cyber Unit, and parallel proceedings on cyberbreaches and incidents by different agencies, branches of government or private litigants.*

Findings – *SEC-regulated entities face many challenges in trying to maintain their ongoing business operations and infrastructure due to severe financial pressures, the threat of infection to employees and customers, and cybersecurity risks posed by remote operations from hackers and fraudsters. The SEC has reemphasized that its long-standing focus on cybersecurity and resiliency within the securities industry will continue, including ongoing vigilance over companies' efforts to identify, assess, and address the inherent, heightened cybersecurity risks of teleworking and the resource reallocation that business need to sustain their operations until a safe and effective vaccine is developed for COVID-19.*

Originality/value – *Expert analysis and guidance from experienced lawyers with expertise in securities, litigation, government enforcement, information technology, data protection, privacy and cybersecurity.*

Keywords *COVID-19 pandemic, U.S. Securities and Exchange Commission (SEC), Teleworking, Cybersecurity, Disclosure obligations, Parallel proceedings*

Paper type *Technical paper*

Aldo M. Leiva (aleiva@bakerdonelson.com) is of counsel in the Fort Lauderdale, Florida, USA office and Michel E. Clark (mclark@bakerdonelson.com) is of counsel in the Houston, Texas, USA office of Baker, Donelson, Bearman, Caldwell and Berkowitz, PC.

The Coronavirus (COVID-19) pandemic has profoundly impacted the operations, finances, and compliance practices of entities regulated by the US Securities and Exchange Commission ("SEC" or "Commission"). Regulated entities face many challenges in trying to maintain their ongoing business operations and infrastructure due to severe financial pressures, the threat of infection to employees and customers, and, within the context of cybersecurity, unique risks posed by remote operations from hackers and fraudsters. COVID-19 has forced companies to rapidly implement remote work operations ("telework") to comply with state-mandated and Centers for Disease Control and Prevention-recommended social distancing requirements to minimize the spread of the virus. The SEC has reemphasized that its long-standing focus on cybersecurity and resiliency within the securities industry will continue, including ongoing vigilance over

companies' efforts to identify, assess, and address the inherent, heightened cybersecurity risks of teleworking and the resource reallocation that businesses need to sustain their operations until a safe and effective vaccine is developed for COVID-19. This article examines the pandemic's effects on regulated entities within the context of cybersecurity [1], SEC compliance, and parallel proceedings (including pending civil litigation tied to allegations of COVID-19-related cybersecurity liabilities).

SEC resiliency and ongoing operations

Throughout the pandemic, the SEC has emphasized its commitment and ability to monitor the securities market. It has issued COVID-19-related guidance, implemented regulatory relief, and continued to investigate and bring enforcement actions to protect investors and the integrity of financial markets [2]. The SEC's ability to conduct its operations within the telework environment was well-documented before the COVID-19 pandemic. For instance, the Office of Personnel Management reported to Congress in 2018 that 91% of SEC staff had worked remotely in 2017 [3]. By March 10, 2020, most SEC staff were teleworking after weeks of transition planning and testing. The SEC adopted a "full telework posture" going forward and various statements were issued by its divisions and offices about how market participants can maintain engagement with SEC staff during this time [4].

COVID-19 cybersecurity-related guidance publications

The Commission's enhanced market monitoring of the adverse effects on regulated companies from COVID-19 was initiated in February 2020 and includes monitoring the "functioning, integrity and resiliency of securities markets with a focus on operations, systems integrity and BCPs [business continuity plans] of US securities clearinghouses, exchanges, other market utilities and key market participants. [5]" In addition to monitoring COVID-19 related issues, the SEC emphasizes that regulated entities should be making robust and focused disclosures about their current and anticipated operations in light of the pandemic, that these disclosures should be non-routine, and that companies should explain the heightened risks they face from the uncertainties of the current environment. The Commission has also repeatedly emphasized the increasing importance of cybersecurity and fraud risks [6].

Public companies

In 2011, the SEC issued its first guidance about disclosure obligations related to cybersecurity risks and incidents [7]. It explained that while no explicit disclosure requirements pertaining to cybersecurity risks and cyber incidents were being imposed, the SEC views the disclosure of cybersecurity risks and issues as consistent with sharing timely and accurate information to help inform investment decisions. As such, cybersecurity disclosures could constitute material information within the context of other required disclosures, and may be necessary to avoid providing misleading information to investors [8]. The 2011 guidance pointed out that public companies should consider the following areas that could trigger specific disclosure obligations (and these areas now may be important for companies to assess their cybersecurity risks and incidents related to COVID-19):

Risk factors

In evaluating their cybersecurity risks, regulated entities must consider prior cyber incidents, their severity and frequency, and assess the probability of cyber incidents along with the anticipated costs and consequences from data breaches, data corruption, or operational disruptions, as well as the adequacy of preventative measures taken reduce cybersecurity risks [9].

Management's discussion and analysis of financial condition and results of operations

Public companies should include cybersecurity risks and incidents in their disclosure discussions if the costs or consequences of such risks and incidents are reasonably likely to materially affect their operations, liquidity, financial condition, future operating results, or financial condition [10].

Description of business

Disclosure of the material effect of cyber incidents on products, services, business relationships, customer relations, or competitive condition may be warranted [11].

Legal proceedings

If a cyber incident gives rise to a material pending legal proceeding, the litigation should be disclosed [12].

Financial statement disclosures

Substantial costs incurred to prevent or mitigate the effects of cyber incidents may need to be included in Financial Statement Disclosures.

Disclosure controls and procedures

If cyber incidents present a risk to a public company's ability to record, analyze, and report information that risk must be disclosed, and the company should consider deficiencies that would render disclosure controls ineffective [13].

In 2018, the SEC updated and expanded upon its 2011 guidance to further aid public companies in preparing disclosures about cybersecurity risks and incidents [14]. The updated guidance emphasized the importance (and required practice) of establishing and maintaining appropriate and effective cybersecurity policies, procedures and disclosure controls to help with accurately and timely disclosing material cybersecurity incidents. The updated guidance underscores that the securities laws' antifraud provisions apply when company directors and officers make "selective disclosures" of nonpublic information about cybersecurity risks or cyber incidents [15].

The emergence of the COVID-19 pandemic resulted in immediate action by the SEC's Division of Corporation Finance, which issued a guidance on March 25, 2020 that provides its views on disclosures and other securities law obligations that regulated companies should be considering [16]. The March 2020 guidance emphasized the continued need for timely and accurate disclosures, especially within the COVID-19 context, as disclosure requirements may apply to a broad range of risks and trigger the disclosure of new or enhanced risks in each of the required categories (i.e., risk factors, business section, management's discussion and analysis, legal proceedings, financial statements, and disclosure controls and proceedings). This guidance includes a footnote that expressly references cybersecurity within this context, stating that "[f]or example, the Commission has highlighted that although no existing disclosure requirement specifically refers to *cybersecurity risks and cyber incidents*, a number of requirements may impose an obligation on companies to disclose such risks and incidents [17]." (Emphasis added). A non-exhaustive list of questions in the guidance provides a potential cybersecurity disclosure checklist [18]:

- How have COVID-19 related cybersecurity risks or cyber incidents impacted the company's financial condition and results of operations?

- How have COVID-19 related cybersecurity risks or cyber incidents impacted the company's capital and financial resources, including its overall liquidity position and outlook?
- Does the company anticipate any material impairments or charges/costs arising out of COVID-19 related cybersecurity risks or cyber incidents to have a material impact on financial statements?
- Have COVID-19-related circumstances such as remote work arrangements (including any related cybersecurity risks or cyber incidents) adversely affected the company's ability to maintain operations, including financial reporting systems, internal control over financial reporting and disclosure controls and procedures?
- Has the company experienced challenges in implementing its business continuity plans (including in regard to cybersecurity or cyber incident prevention/response) or does it foresee requiring material expenditures to do so?

In light of the difficulty that regulated companies face in assessing trends or addressing the uncertainties from COVID-19 and its multiple impacts on business operations and outlook, the Division of Corporation Finance emphasizes that forward-looking information may be used to convey information to investors and that companies should use the available safe harbors when making these disclosures [19]. Consistent with the updated guidance issued in 2018, the March 2020 guidance also repeats that company directors, officers, and insiders must refrain from trading in the company's securities when a material risk to investors emerges, but has not yet been publicly disclosed. Companies and their officers must also "avoid selective disclosures" when disseminating the pertinent information [20]. On June 23, 2020, the Division of Corporation Finance issued an additional COVID-19 guidance pertaining to operations, liquidity, and capital resources disclosures that should be considered with respect to business and market disruptions related to COVID-19 [21]. While the guidance did not refer or cite to cybersecurity issues, it should be reviewed in assessing cybersecurity risks or incidents if they present a material operational challenge or impact or are reasonably likely to impact a business's financial condition and liquidity.

SEC-Regulated entities

In addition to the cybersecurity guidances directed toward public companies, the SEC's Office of Compliance Inspections and Examinations (OCIE) has issued publications directed toward broker-dealers and investment advisories. In 2015, the OCIE launched its cybersecurity examination initiative, which builds on earlier examinations. It further assesses the cybersecurity preparedness in the securities industry, and includes a focus on the management of cybersecurity risks associated with third-party vendors of SEC-regulated entities [22]. In 2018, the OCIE issued its 2018 National Exam Program Examination Priorities, which communicated a continued prioritization of cybersecurity in each of its examination programs [23].

On January 27, 2020, weeks before the first COVID-19 cases were reported in the United States, the OCIE published its "Cybersecurity and Resiliency Observations" Report as part of this continuing trend on cybersecurity issues. This report provides OCIE's observations of industry best practices and cybersecurity approaches "to assist market participants in their consideration of how to enhance cybersecurity preparedness and operational resiliency [24]." Issued only 15 days before the World Health Organization's declaration of the COVID-19 global pandemic [25], the OCIE report provides the most recent analysis of cybersecurity practices by regulated entities. While not binding, the OCIE's observations are intended to help enhance cybersecurity efforts by market participants subject to its audits and addresses the following areas of cybersecurity:

- governance and risk management;
- access rights and controls;

- data loss prevention;
- mobile security;
- incident response and resiliency;
- vendor management; and
- training and awareness.

OCIE's observations should serve as a guide for assessing, updating, or implementing COVID-19-related cybersecurity controls.

Governance and risk management

In assessing the maturity and effectiveness of cybersecurity governance [26], the OCIE identified such common features as:

- performance of risk assessments to identify, analyze, and prioritize cybersecurity risks to the organization; and
- drafting, implementation, and enforcement of written cybersecurity policies and procedures to address those risks.

It observed that significant numbers of board members and senior management should be involved in providing successful plans to anticipate, identify, and address cybersecurity issues. Within the context of COVID-19, updated risk assessments should identify specific vulnerabilities and threats associated with telework. Based on the results of such assessments, policies and procedures that had been reserved for emergency or business continuity operations may be applied and, if required, drafted and implemented to address specific operational cybersecurity hazards and threats associated with COVID-19. For example, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has warned companies and employees working remotely to take precautions against cybercriminals by exercising caution in opening or reviewing any emails with a COVID-19-related subject line, attachment, or hyperlink, as well as in responding to any social media pleas, text messages, or phone calls related to COVID-19 [27]. The Department of Justice has similarly issued warnings related to reports of phishing emails posing as the World Health Organization or the Centers for Disease Control and Prevention, and malicious websites and apps purporting to share virus-related information in order to gain access to devices and/or cause recipients to download malware or ransomware [28]. Against these and other warnings, regulated entities should be considering the adequacy of their existing policies, procedures, and employee training materials to address these specific COVID-19-related threats.

Access rights and controls

OCIE also identified several controls implemented to ensure proper user rights and access to company systems, namely [29]:

- identifying the location of data throughout the organization;
- restricting access to such data to authorized users; and
- establishing appropriate controls to prevent and control for unauthorized access.

These measures should be coupled with effective monitoring of the organization's data and its transfer. As business operations have expanded to employees' home networks, company data now is potentially accessible not only through company-issued laptops and mobile devices, but also via personal laptops and mobile devices. Even in situations where companies have instructed employees to log into company systems via virtual private networks ("VPNs"), known exploits of VPN vulnerabilities may allow hackers and cybercriminals to access company

data [30]. For this reason, CISA issued a cybersecurity alert focusing on VPN security that includes recommended measures, such as updating VPNs and network infrastructure devices, implementing multi-factor authentication on all VPN connections and the use of strong passwords, ensuring that the cybersecurity team is prepared to ramp up tasks to address home network vulnerabilities, and updating incident response/recovery plans to include telework environments [31]. The OCIE Report encourages regulated entities to register for CISA cybersecurity alerts as an additional resource for tracking cybersecurity threats [32]. Regulated entities should be registering for such alerts, while assessing and updating access rights and controls, as indicated.

Data loss prevention

OCIE also notes the use of technical systems and monitors to prevent data loss [33], such as:

- vulnerability scanning;
- perimeter security;
- detective security;
- patch management;
- inventory of hardware and software;
- encryption and network segmentation;
- insider threat monitoring; and
- securing legacy systems and equipment.

Such systems should be consistently reevaluated to maintain consistency with new practices and evolving cyber threats. In addition, employees should also be cautioned against sending non-public information to personal email accounts and devices [34], especially usernames or passwords allowing access to company VPNs or systems.

Mobile security

Recognizing the widespread and ever-increasing use of mobile devices, the OCIE notes that additional cybersecurity challenges created by their adoption warrants the following practices [35]:

- implementing appropriate policies and procedures for mobile devices;
- managing the use of mobile devices, including a mobile device management application;
- implementing security measures; and
- employee training.

Given the central role of mobile devices such as laptops, tablets, and smartphones for remote access in teleworking, companies should assess the risks of employees using personal laptops/devices that lack security features of company-issued laptops/devices. Similarly, telework policies and procedures should be modified as necessary to address the primary role of telework in sustaining business continuity [36].

Incident response and resiliency

As cyber incidents can occur despite adopting sophisticated and comprehensive control measures and policies, the OCIE notes the importance of an incident response program that includes:

- identifying applicable cybersecurity breach reporting requirements to state and local authorities;
- articulating response team roles and responsibilities; and
- testing of the program and its plans [37].

Within the context of COVID-19, as part of their ongoing assessment of telework vulnerabilities, regulated entities should review incident response plans, including the reporting of significant cyber incidents to federal authorities to mitigate against broad impacts to national security and economic security [38]. In addition, victims of cybercrimes or attempted fraud involving COVID-19 may notify the FBI at tips.fbi.gov or [39], if a cyber scam is involved, may submit a complaint through the Internet Crime Complaint Center's portal at www.ic3.gov

Vendor management

Because many companies rely on third-party vendors for key data-related services (such as data hosting or software-as-a-service solutions), and vendors may present substantial risks to regulated entities, several measures should be adopted [40]:

- due diligence during the vendor selection process;
- consistent monitoring and management of vendor performance and compliance with contractual terms;
- assessing vendor relations to monitor the risk assessment process; and
- monitoring of vendors' data protection measures and their client information.

A robust vendor management program should ensure compliance with applicable company standards and cybersecurity practices and place a special focus on COVID-19 threat mitigation – which may also be assessed in conjunction with self-assessment by a regulated entity [41].

Training and awareness

OCIE has also identified employee training and cybersecurity awareness as key compliance features used by many organizations, namely [42]:

- policies and procedures mandating training;
- inclusion of concrete examples and fact-specific exercises as part of such training; and
- measuring training effectiveness.

As part of its Risk Management for Novel Coronavirus bulletin, CISA includes enhanced employee training on personal and worksite protection strategies, which includes cybersecurity considerations within the COVID-19 context [43]. Shortly after this OCIE report was issued and news of an impending global pandemic started circulating, SEC Chairman Clayton issued a statement on January 30, 2020 directing SEC staff to monitor issuer disclosures and providing guidance on the effects of COVID-19 to investment decisions in the market [44]. Clayton's statement was followed by a series of statements and guidances from February through June 2020 (as of the time of this article) focusing on COVID-19's effects on specific aspects of operations – among which was a March 17, 2020 update on the consolidated audit trail ("CAT"), a temporary COVID-19 Staff no action letter, and reducing CAT-related cybersecurity risks [45].

SEC cybersecurity enforcement actions and activities

Under its civil enforcement authority, the SEC is authorized to bring cybersecurity-related enforcement actions to protect investors, punish regulated entities that do not adhere to reasonable cybersecurity measures (such as those identified in the OCIE report), and deter future violations [46]. The Division of Enforcement's Cyber Unit was established in September 2017 to focus on violations involving digital assets, including coin offerings and cryptocurrencies, cybersecurity controls, disclosures of cybersecurity incidents and risks by issuers, insider trading based on hacked nonpublic information, and other cybersecurity issues, such as brokerage account takeovers and market manipulations via electronic platforms [47]. With the onset of the pandemic, the SEC has announced its focus on maintaining enforcement and investor protection efforts [48]. On March 23, 2020, the Division of Enforcement issued a statement emphasizing the "importance of market integrity and following corporate controls and procedures" during the COVID-19 pandemic [49]. As discussed, cybersecurity risk and incidents are among the areas that must be assessed and included in corporate controls and procedures, especially as to disclosure requirements. While the SEC has not announced an enforcement action addressing cybersecurity within the context of COVID-19 [50], its history of ever-increasing focus on cybersecurity issues in its enforcement and activities provides timely and useful information for companies to better assess cybersecurity risks, relevant policies and procedures, and action/response plans in the face of increased cybersecurity risks in the COVID-19 environment. As CISA emphasized in its April 8, 2020 Joint Alert that warns about COVID-19 exploitation by malicious cyber actors (and aligns with the cybersecurity concerns raised in the OCIE guidance publications) [51], the use of phishing, malware distribution, and cyber-attacks against newly or rapidly deployed remote access and teleworking infrastructure pose serious risks. The enforcement actions described below provide an overview of the various fact patterns and risk factors that have led to SEC enforcement action in the past, as cybersecurity will likely be a focus of SEC enforcement action and activities in the COVID-19 environment.

On April 24, 2018, shortly after launching its Cyber Unit, the SEC announced a $35 Million settlement with Altaba (formerly Yahoo! Inc.) related to Altaba's failure to timely disclose a December 2014 data breach in which Russian hackers stole personal data related to more than 500 million user accounts [52]. The Commission explained that despite learning of the data breach within days of its occurrence, Altaba's senior management and its legal department failed to conduct a proper investigation and consider whether the breach should be publicly disclosed. The breach went unreported until September 2016, at which point Yahoo was closing the acquisition of its operating business by Verizon Communications, Inc. Altaba neither admitted or denied the findings in the SEC's order, which also required it to cease and desist from further violations of applicable securities laws [53]. Within the COVID-19 context, as bad actors continue their efforts to infiltrate company computer systems via home computers, employer-provided laptops, and devices used for teleworking, the timely detection and assessment of potential data breaches should remain a top priority for public companies and regulated entities.

On September 26, 2018, the SEC also announced that regulated entity Voya Financial Advisors, Inc. ("Voya') agreed to pay a $1,000,000 fine to settle charges arising from an April 2016 cyber incident that compromised customer information [54]. This was the first-ever SEC enforcement action of its Identity Theft Red Flags Rule ("Red Flags Rule") and provides a useful overview of procedural flaws and missteps by Voya that led to several violations of the Red Flags Rule and payment of the fine. The settlement concluded an SEC investigation triggered by an April 2016 series of incidents in which persons impersonating Voya contractor representatives called a technical support line to request a reset of various account passwords, despite using phone numbers that Voya had previously identified as associated with fraud activity [55]. Voya's technical support staff reset the passwords and

even provided a username on one occasion. Within three hours, a legitimate Voya contractor representative reported that his password had been changed, despite not having requested a reset. The perpetrators continued these practices over several days, culminating in unauthorized access to at least 5,600 customer accounts and obtaining account documents for at least one customer [56]. Although no unauthorized transfer of funds or securities took place, the SEC initiated its investigation into Voya's compliance with the Identity Theft Red Flags Rule, a regulation that requires financial services companies to adopt measures to prevent identity theft in new and existing accounts. Specifically, the rule requires adoption of written policies and procedures to address administrative, technical, and physical safeguards for the protection of customer records and information, and "must be reasonably designed to:

- insure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer [57].

The settlement order also provides a useful overview of specific violations cited by the SEC against Voya [58], which should be considered carefully by any company subject to SEC enforcement or regulatory action, and include:

- Failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule");
- Failure to develop and implement a written Identity Theft Prevention Program as required by Rule 201 of Regulation S-ID (17 C.F.R. § 248.201) (the "Identity Theft Red Flags Rule");
- Deficient policies and procedures prior to the incident, such as policies and procedures that were not reasonably designed to apply to systems used by Voya contractor representatives and issuance of temporary passwords via unsecured email, among others;
- Deficient response to the incident, with passwords continuing to be reset via telephone for several days, despite Voya having issued a new policy to discontinue the practice, following first notification of the unauthorized password change by a legitimate Voya contractor representative; and
- Initial failure to block IP addresses associated with fraudulent activity and accepting calls from phone numbers that were on a designated "monitoring list".

The SEC also mentioned specific remedial efforts taken by Voya [59], which were taken into consideration in settling the matter:

- Blocking malicious IP addresses;
- Revising policies to prohibit communication of temporary passwords by phone;
- Issuing breach notices to affected customers, describing the incident and offering one year of free credit monitoring; and
- Naming a new Chief Information Security Officer to create and maintain cybersecurity policies and procedures.

The civil settlement, which requires a consultant to oversee Voya's compliance with the Red Flags Rule, underscores that regulated companies must fully comply with the Safeguards Rule and the Red Flags Rule [60], especially in the COVID-19 environment where bad

actors may use tactics such as those successfully used against Voya employees. A month after announcing the Voya settlement, SEC's Division of Enforcement issued a Report of Investigation about multiple business email compromises and explained how fraudsters posing as high-level company executives or vendors had sent fraudulent emails to company personnel that duped them into transmitting large wire transfers to bank accounts they controlled [61]. The investigation assessed whether the victim companies had violated federal securities laws by failing to sufficiently include cyber threats in their internal accounting controls. While the Division of Enforcement did not recommend enforcement action, its report cautions public companies to consider cyber threats when implementing internal accounting controls [62].

Public companies and regulated entities must be continually assessing their policies and procedures, including the training for remote employees on these risks for the foreseeable future because of the continued use of attempted business email compromises in the COVID-19 environment, such as the issuance of fraudulent emails with references to COVID-19 information, claims, or products [63]. As the history and ongoing attention to cybersecurity within the COVID-19 context shows, regulated entities should be conducting ongoing assessments of cybersecurity risks and incidents and familiarize themselves with the SEC's enforcement history related to cybersecurity.

Parallel proceedings

As noted, the SEC has identified serious risks that regulated companies and investors face from cyberbreaches and incidents. These risks are becoming increasingly important during the pandemic since, as noted, such a large percentage of the workforce is teleworking, which creates more opportunities for bad actors to exploit systemic weaknesses in cybersecurity protections. As also noted, the Commission seeks to protect the securities markets and the investing public by educating market participants, imposing disclosure duties upon publicly traded entities, and prohibiting fraud, manipulation, and insider trading (Clark, 2006). Violations of these duties increasingly result in parallel proceedings and their threats of significant fines, penalties, restitution orders, and other collateral consequences, including reputational damage.

The term "parallel proceedings" refers to the simultaneous or successive investigation of criminal, civil and administrative actions by different agencies, branches of government, or private litigants involving the same party and facts. *See Securities and Exchange Commission v. Dresser Industries,* 628 F.2d 1368 (D.C. Cir.) (*en banc*), *cert. denied,* 449 US 993 (1980). Parallel actions may involve agency administrative enforcement actions [64], civil lawsuits (including class actions and shareholder derivative suits), and criminal actions. As has been pointed out, "[s]uccessful cyber-attacks lead to millions of dollars in remediation costs and can create many forms of legal liability for a company. These liabilities and costs can have serious repercussions on the value of a business, which ultimately can negatively affect a stockholder. This harm has invariably led to the rise of derivative liability for a corporation's Board of Directors, which can force them to incur personal damages (Dynkin and Dynkin, 2017)." The board may face personal liability threats for allegedly violating their oversight responsibilities [65].

The threat of parallel proceedings requires careful coordination. Not only are they costly and disruptive, but a making a misstep in handling related proceedings (or threatened actions) can result in waived privileges, admissions, and collateral estoppel problems. The need to develop, implement, and update robust cybersecurity measures also present practical issues that listed companies must address when fulfilling their responsibilities. While having an outside expert make an internal risk assessment and conduct penetration tests as part of that assessment to measure the effectiveness of a company's cybersecurity program may make sense for complying with the SEC's (and other) cybersecurity directives, compliance activities may not be shielded by cognizable legal privileges and

may result in unintended consequences. An "internal risk assessment requires companies to do the following tasks:

- provide network vulnerability assessments;
- provide recommendations to remediate potential vulnerabilities;
- review its cyber policies and procedures; and
- review its internal network [66].

Depending on how these tests are set up and performed, the consulting agent's findings may not be privileged. Worse still, the consultant's report could provide a roadmap that helps a plaintiff's counsel support claims that the company's cybersecurity measures were so deficient that it breached duties owed to the plaintiff (or class of plaintiffs) and caused foreseeable damages. This problem can be very real for companies trying to ensure that they have robust cybersecurity protections by having internal risks assessments performed by outside consulting experts if they do not anticipate the problems of how to best protect the findings from conducting those risk assessments by properly structuring the engagement to try to protect the findings as privileged.

These practical problems are addressed in a recent district court case, *In re Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA), 2020 WL 3470261 (E.D. VA June 25, 2020) (Slip Copy). While *In re Capital One* is not a pure parallel proceeding scenario, the same principles and risks central to this decision apply to companies facing similar risks. The federal district judge in *In re Capital One* adopted a Magistrate-Judge's recommendation to reject the large bank's assertion of the work product doctrine privilege to protect its cybersecurity consultant's report from discovery in a class action [67].

A brief overview of this matter is illustrative. Capital One had entered into a Master Services Agreement with FireEye, Inc., d/b/a Mandiant ("Mandiant") that included various Statements of Work so that Capital One could respond quickly to a cybersecurity incident [68]. Under the Statements of Work, Mandiant agreed to provide incident response services (computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance), a final report, and, if necessary, a written technical document outlining the results and recommendations for remediation [69]. In 2019, a breach happened. Capital One retained Debevoise & Plimpton LLP for legal advice regarding the incident and Debevoise, in turn, signed an agreement with Mandiant to provide services and advice, as directed by counsel *for the same scope of work* that Mandiant already had agreed to provide to Capital One in an earlier Statement of Work [70]. This proved to be problematic to Capital One's later assertion of privilege.

After Debevoise executed the agreement with Mandiant (which referenced Mandiant's 2015 agreement with Capital One and required it to abide by that agreement's terms), Capital One, Mandiant, and Debevoise executed an addendum to the agreement to ostensibly expand the engagement to include "penetration testing of systems and endpoints [71]." When Mandiant issued its report, it was sent to Debevoise. In turn, Debevoise sent the report directly or at Capital One's direction to Capital One's legal department, its Board of Directors, its financial regulators, its outside auditor, and dozens of its employees [72]. Mandiant's payments came from Capital One's negotiated budget set out in its 2019 Statement of Work; after that was exhausted, it was paid from funds in Capital One's Cyber budget – which the business later re-designated as "legal expenses [73]." While Debevoise's engagement of Mandiant ordinarily would appear to have protected the assertion of the work product doctrine's protection for the Mandiant's report to Debevoise so that it could advise its client about legal issues arising from the cyberbreach, the judge seized on the law firm's reference in its engagement with Mandiant to the earlier agreement between Capital One and Mandiant as one of the reasons for

rejecting Capital One's assertion of the work product doctrine to prevent the plaintiffs from obtaining the report. [74]

The basic takeaway from *In re Capital One* is that listed companies should be consulting with counsel about what can be done to establish and maintain available privileges when implementing common cybersecurity measures since there are many ways in which such protections can be waived or not available when they are needed.

Conclusion

Companies regulated by the Commission must navigate through a web of duties and requirements in order to take advantage of the opportunities provided by the capital markets. An increasingly important component of their responsibilities is to provide robust cybersecurity compliance measures to protect the company and its investors from bad actors. The pandemic has exacerbated the pressures faced by listed companies and cybersecurity has become even more important. What constitutes appropriate, robust cybersecurity measures is somewhat fluid since fraudsters and other bad actors, including foreign countries, regularly try to breach security systems to steal monies, intellectual property, and other valuable assets from businesses. In light of their oversight responsibilities, companies' boards of director cannot take a "business as usual" approach when it comes to their oversight duties, particularly in these trying times, and particularly as to cyber-preparedness measures. While the pandemic will eventually end, its lasting impact likely will increase what is required for businesses to satisfy the SEC and others that they have implemented appropriately robust cybersecurity measures, and perhaps may lead the SEC to promulgate a formal duty for listed businesses (and those who are charged with their oversight) to meet basic cybersecurity standards – which regulatory duty would result in far more cybersecurity litigation.

Notes

1. While beyond the scope of this article, regulated entities may be subject to additional federal and/or state cybersecurity laws and regulations, depending on their service offerings, data collection practices, and scope of operations. Among the US laws relied upon by federal authorities to govern cybersecurity are the Gramm-Leach-Bliley Act (which also applies to securities firms and is also one of the laws enforced by the SEC), the Federal Trade Commission Act, the Health Insurance Portability and Accountability Act, and, at the state level, individual state data breach notification laws (some of which reference "reasonable" cybersecurity controls), including the California Consumer Privacy Act of 2018 (enforceable as of July 1, 2020, which includes a private cause of action of California consumers for the breach of unencrypted personal data resulting from a violation of the duty to implement and maintain reasonable security procedures and practices) and the New York State Department of Financial Services (23 NYCRR 500) CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES (which include adoption and implementation of a robust cybersecurity program). Multinational entities may be subject to foreign laws relating to cybersecurity practices, including the European Union's General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) and dozens of other data protection laws that address cybersecurity practices and safeguards.
2. *See* www.sec.gov/sec-coronavirus-covid-19-response (accessed 5/18/20).
3. *See* US Office of Pers. Mgmt., Status of Telework in the Federal Government, 89, 94, and 142 (2019).
4. *See* www.sec.gov/sec-coronavirus-covid-19-response, "Agency Operations: Transition to Telework and Continuity of Operations" (accessed 5/18/20).
5. *See* www.sec.gov/sec-coronavirus-covid-19-response, "Market Monitoring and Engagement with Market Participants" (accessed 5/18/20).
6. *See* Cybersecurity & Infrastructure Sec. Agency, US Dep't of Homeland Sec. & UK Nat'l Cyber Sec. Ctr., Alert: COVID-19 Exploited by Malicious Cyber Actors (Apr. 8, 2020) https://us-cert.cisa.gov/ncas/alerts/aa20-099a (accessed 7/26/20).

7. *See* CF Disclosure Guidance: Topic No. 2 (10/13/11), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (accessed 7/26/20).
8. *See* Securities Act Rule 408 and Exchange Act Rules 12b-20 and 14a-9; *Basic Inc. v. Levinson*, 485 US 224 (1988); and *TSC Industries, Inc. v. Northway*, Inc., 426 US 438 (1976) (Information is "material" if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or it would significantly alter the total mix of information available by the disclosing entity). The antifraud provisions of the federal securities laws apply to statements and omissions both inside and outside Commission filings. *See* Securities Act §17(a); Exchange Act § 10(b); and Exchange Act Rule 10b-5.
9. CF Disclosure Guidance: Topic No. 2 (10/13/11) states that appropriate disclosures may also include (1) a discussion of aspects of the company's business or operations that may give rise to cybersecurity risks and related potential costs and consequences, (2) if outsourced functions have material cybersecurity risks, a description of how such risks are addressed, (3) a description of cyber incidents experienced by the company, including resulting costs and consequences, (4) identification of the risks related to undetected cyber incidents, and (5) a description of applicable insurance coverage.
10. *See* CF Disclosure Guidance: Topic No. 2 (10/13/11), note 6, citing Item 303 of Regulation S-K; and Form 20-F, Item 5; Commission Guidance Regarding Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8350 (Dec. 19, 2003) [68 FR 75056]; Commission Statement about Management's Discussion and Analysis of Financial Condition and Results of Operations, Release No. 33-8056 (Jan. 22, 2002) [67 FR 3746]; and Management's Discussion and Analysis of Financial Condition and Results of Operations; and Certain Investment Company Disclosures, Release No. 33-6835 (May 18, 1989) [54 FR 22427].
11. *See* CF Disclosure Guidance: Topic No. 2 (10/13/11), note 7, citing to Item 101 of Regulation S-K and Form 20-F, Item 4.B.
12. *See id.*, note 8, citing to Item 103 of Regulation S-K.
13. *See id.* note 11, citing to Item 307 of Regulation S-K; and Form 20-F, Item 15(a).
14. *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures (2/26/18), *available at*: https://www.sec.gov/rules/interp/2018/33-10459.pdf
15. *Id* at p. 7.
16. *See* CF Disclosure Guidance: Topic No. 9 (3/25/20), www.sec.gov/corpfin/coronavirus-covid-19 (accessed 7/26/20).
17. *See id* note 2, citing to Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018), *available at*: www.sec.gov/rules/interp/2018/33-10459.pdf
18. Adapted from the general disclosure checklist contained in CF Disclosure Guidance: Topic No. 9 (3/25/20).
19. *See* CF Disclosure Guidance: Topic No. 9 (3/25/20), referencing safe harbors under Section 27A of the Securities Act and Section 21E of the Exchange Act.
20. *See id.* note 4, citing to Regulation FD 17 CFR 243.100, *et seq.* and Selective Disclosure and Insider Trading, Release No. 33-7881 (Aug. 15, 2000).
21. *See* Disclosure Guidance: Topic 9A (6/23/20), *available at*: www.sec.gov/corpfin/covid-19-disclosure-considerations
22. *See* OCIE National Exam Program Risk Alert, Volume IV, Issue 8 (9/15/2015) , *available at*: www.sec.gov/files/ocie-2015-cybersecurity-examination-initiative.pdf
23. *See* OCIE 2018 National Exam Program Examination Priorities www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf
24. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 2 (accessed 5/18/20).
25. *See* https://www.washingtonpost.com/health/2020/03/11/who-declares-pandemic-coronavirus-disease-covid-19/ (accessed 5/18/20).
26. *See* https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 2 (accessed 5/18/20).
27. *See* www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams (accessed 5/18/20).

28. *See* https://www.justice.gov/coronavirus (accessed 5/18/20).
29. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 3 (accessed 5/18/20).
30. *See* www.us-cert.gov/ncas/alerts/aa20-133a, "Top 10 Routinely Exploited Vulnerabilities" (accessed 5/18/20).
31. *See* www.us-cert.gov/ncas/alerts/aa20-073a (accessed 5/18/20).
32. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 8 (accessed 5/18/20).
33. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 4 (accessed 5/18/20).
34. *See, e.g.*, New York Department of Financial Services, Guidance to Department of Financial Services ("DFS") Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic, April 13, 2020 www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness (accessed 5/18/20).
35. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 6 (accessed 5/18/20).
36. *See, e.g.*, www.us-cert.gov/ncas/alerts/aa20-073a (accessed 5/18/20).
37. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 6 (accessed 5/18/20).
38. *See, e.g.* "Cyber Incident Reporting, A Unified Message for Reporting to the Federal Government," *available at*: www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
39. *See e.g.,* www.fbi.gov/investigate/cyber (accessed 5/18/20).
40. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 8 (accessed 5/18/20).
41. *See, e.g.*, New York Department of Financial Services, Guidance to Department of Financial Services ("DFS") Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic, April 13, 2020, *at* www.dfs.ny.gov/industry_guidance/industry_letters/il20200413_covid19_cybersecurity_awareness (accessed 5/18/20).
42. *See* www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf, p. 9 (accessed 5/18/20).
43. *See* www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf (accessed 5/18/20).
44. *See* www.sec.gov/news/public-statement/clayton-mda-2020-01-30 (accessed 5/18/20).
45. *See* www.sec.gov/news/public-statement/statement-clayton-cat-covid-19-nal-cybersecurity-2020-03-17 (accessed 5/18/20).
46. Under its general enforcement authority over Regulation S-P (which requires broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information," Release 34-42974, Privacy of Consumer Financial Information (Regulation S-P), Section III, Subpart E - Safeguard Procedures (June 22, 2000)), the SEC had previously undertaken enforcement actions against RT Jones Capital Equities Management, Inc. (2015), (for not safeguarding customer data from cyber-breaches in violation of Reg S-P by storing sensitive customer information on a third-party hosted web server that was hacked and its failure to adopt written policies and procedures reasonably designed to safeguard such customer information) www.sec.gov/news/pressrelease/2015-202.html. *See also* Morgan Stanley Smith Barney, LLC (2016), where the Commission brought an enforcement action against the large brokerage firm for not safeguarding customer data from cyber-breaches in violation of Reg. S-P, tied to a Morgan Stanley employee who transferred confidential customer data to a personal server that was eventually hacked (www.sec.gov/news/pressrelease/2016-112.html)
47. *See* Press Release 2017-176, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), *available at*: www.sec.gov/news/press-release/2017-176
48. *See* SEC Coronavirus Response, *available at*: www.sec.gov/sec-coronavirus-covid-19-response

49. *See* Statement from Stephanie Avakian and Steve Peikin, Co-Directors of the SEC's Division of Enforcement, Regarding Market Integrity (March 23, 2020), *available at*: www.sec.gov/news/public-statement/statement-enforcement-co-directors-market-integrity

50. To-date, the SEC's enforcement actions brought in connection with COVID-19 related issues have involved the Commission's rapid response to frauds, illicit schemes, and other misconduct affecting investors – such as schemes involving false assertions about the purported availability/offerings of COVID-19 blood tests, thermal scanning equipment, and personal protective equipment. There have also been trading suspensions related to such conduct. *See* Note 48, at the tab entitled "Enforcement, Examinations, and Investor Education".

51. *See* Note 6.

52 *See* Press Release 2018-71, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (April 24, 2018), *available at*: www.sec.gov/news/press-release/2018-71

53. *Id.*; See specifically, Securities Act §§17(a)(2) and 17(a)(3) and Exchange Act § 13(a), as well as Rules 12b-20, 13a-1, 13a-11, 13a-13, and 13a-15.

54. *See* Press Release 2018-213, SEC Charges Firm with Deficient Cybersecurity Procedures (Sept. 26, 2018), *available at*: www.sec.gov/news/press-release/2018-213

55. *See* Order Instituting Administrative and Cease-and-Desist Proceedings In the Matter of Voya Financial Advisors, Inc. (September 26, 2018), *available at*: www.sec.gov/litigation/admin/2018/34-84288.pdf

56. *Id.*

57. *See* Procedures to Safeguard Customer Records and Information; Disposal of Consumer Report Information, 17 CFR § 248.30 [65 FR 40362, June 29, 2000, as amended at 69 FR 71329, Dec. 8, 2004].

58. *See* Note 51.

59. *Id.*

60. *Id.*

61. *See* Press Release 2018-236, SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls (Oct. 16, 2018), *available at*: www.sec.gov/news/pressrelease/2018-236

62. *See* October 2018 SEC Business Email Fraud Investigative report www.sec.gov/litigation/investreport/34-84429.pdf

63. *See* Note 6.

64. Another development that could impact the cybersecurity area is the growing number of successful whistleblower actions being submitted to the SEC's Office of the Whistleblower, which was enacted in 2011. The SEC's whistleblower program has been very successful and many plaintiffs' counsel who represent whistleblowers in *qui tam* suits filed in the name of the United States under the applicable provisions of the federal civil False Claims Act (see 31 U.S.C. § 3730 (b)), in the hope of obtaining a percentage of the statutory damages for their clients have expanded their practices to represent SEC whistleblowers. Having a financially motivated whistleblower with inside knowledge of wrongdoing by regulated businesses creates a host of dangers to listed companies.

65. While beyond the scope of this article, the so-called "Caremark doctrine" recognizes that the failure of directors to meet basic oversight responsibilities to the company could result in personal liability for members of its board of directors. *See, e.g., In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996) and *McCall v. Scott,* 239 F.3d. 808 (6th Cir. 2001). As one scholar explains, "Corporate law, buttressed by securities law, imposes upon directors and officers a fiduciary *duty of care*, which often manifests itself in the form of a monitoring function. For directors, a duty to monitor corporate affairs stems from the principle that all corporate affairs must be managed under the direction of the board of directors." Lisa M. Fairfax, *The Sarbanes-Oxley Act as Confirmation of Recent Trends in Director and Officer Fiduciary Obligations,* 76 St. John's L. Rev. 953, 954 (2002) (internal notes omitted).

66. Karen Painter Randall and Steven A. Kroll, "Protecting Data Security Risk Assessments from Disclosure in Subsequent Breach Litigation," USLAW (FALL/WINTER 2017).

67. The work product doctrine, articulated by the Supreme Court in *Hickman v. Taylor*, 329 US 495 (1947), provides that any notes, working papers, memoranda or similar materials prepared by an

attorney in anticipation of litigation are protected from discovery. *See also* Fed. R. Civ. Proc. 26(b)(3). Federal courts do not recognize the breadth of privileges that state courts do, particularly when it comes to compliance activities. For example, federal courts do not recognize the self-evaluative privilege to protect from discovery compliance reviews performed by a business to address its compliance with laws, rules and regulations. *See Bredice v. Doctors Hosp. Inc.*, 50 F.R.D. 249 (D.C. 1970), *aff'd w/o opinion,* 479 F.2d 920 (D.C. Cir. 1973).

68. *In re Capital One*, 2020 WL 3470261 at *1.
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.* at *2.
73. *Id.* at *2.
74. *Id.* at *5.

References

Clark, M.E. (2006), "The growing importance of securities regulation for publicly traded entities in the post-Sarbanes-Oxley marketplace", Health Law and Compliance Update §5.01 (internal notes omitted).

Dynkin, B. and Dynkin, B. (2017), "Derivative liability in the wake of a cyber attack", *Albany law Journal of Science and Technology*, Vol. 23.

Corresponding author

Aldo M. Leiva can be contacted at: aleiva@bakerdonelson.com