MAYER | BROWN

October 15, 2021

Legal Update

US Securities and Exchange Commission Increases Focus on Cybersecurity

This past summer's string of cyber enforcement actions signals that cybersecurity has become a top priority for the US Securities and Exchange Commission ("SEC"). This focus is consistent with the SEC's Division of Examinations annual examination priorities, which have consistently included information security for the past several years. In particular, the 2021 examination priorities provided that the division would "review whether registrants have taken appropriate measures to: safeguard customer accounts and prevent account intrusions, including verifying an investor's identity to prevent unauthorized account access; oversee vendors and service providers; address malicious email activities, such as phishing or account intrusions; respond to incidents, including those related to ransomware attacks; and manage operational risk as a result of dispersed employees in a work-from-home environment."[1] The SEC's continued focus on securities law violations related to cybersecurity is also in alignment with its 2018 Guidance on Public Company Cybersecurity Disclosures.[2]

On August 30, 2021, the SEC announced three separate actions sanctioning eight broker dealers and/or investment advisory firms for deficiencies in their cybersecurity policies and procedures.[3] The SEC announced that these firms experienced email account compromises that led to the potential exposure or exfiltration of personally identifiable information ("PII") of thousands of customers or clients for each firm. In the SEC's announcement, Kristina Littman, chief of the SEC Enforcement Division's Cyber Unit, stated that "[i]t is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks."[4]

Just two weeks earlier, the SEC announced that Pearson plc ("Pearson"), a London-based educational publishing and services company, agreed to pay $1 million to settle charges that it misled investors about a 2018 data breach involving millions of student records and had inadequate disclosure controls and procedures.[5]

These enforcement actions highlight the SEC's attention to cybersecurity and its scrutiny of written documentation and disclosures following incidents. In this National Cybersecurity Awareness Month Legal Update, we discuss the SEC's recent cyber enforcement actions, as well as key lessons that SEC registrants may consider in augmenting their own risk management posture and communicating breaches to investors and clients.

Actions Charging Deficient Cybersecurity Procedures

BACKGROUND

Section 504 of the Gramm-Leach-Bliley Act of 1999 ("GLBA") required the federal financial services regulators (including the SEC) to adopt regulations implementing the GLBA's requirements regarding the safeguarding of customer information.[6] The SEC subsequently adopted a rule requiring the safeguarding of customer information ("Safeguards Rule"), which requires every broker-dealer and every investment adviser registered with the SEC to adopt "written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information" reasonably designed to:

1) Ensure the security and confidentiality of customer records and information;
2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[7]

The Safeguards Rule also requires subject entities to "properly dispose of [consumer report] information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."[8]

The eight firms charged by the SEC on August 30, 2021, included Cetera Advisor Networks LLC, Cetera Advisors LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC and Cetera Investment Advisers LLC ("Cetera Entities"); Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc. ("Cambridge"); and KMS Financial Services, Inc. ("KMS").[9] Specifically, the SEC charged these firms with violations of the Safeguards Rule, alleging that the firms failed to adopt required written policies and procedures to secure and protect customer information.[10] The SEC also found that two of the Cetera Entities, Cetera Advisors LLC and Cetera Investment Advisers LLC, violated Section 206(4) of the Advisers Act and associated Rule 206(4)-7 by sending misleading breach notifications to clients.[11]

In each of these actions, the SEC noted that the email account compromises did not appear to have resulted in unauthorized trades or transfers from customer accounts. The SEC also considered mitigation measures that the firms took in determining the appropriate penalties. In each action, the firms settled without admitting fault and will pay penalties ranging from $200,000–$300,000.

CETERA ENTITIES

In the action announced against the Cetera Entities, the SEC alleged that over 60 employee email accounts for Cetera Entities were compromised, resulting in the exposure of over 4,388 of customers' PII stored in those accounts. The SEC also alleged that, at the time, these accounts did not have multi-factor authentication ("MFA") enabled, in violation of the Cetera Entities' own policies, which had required MFA "wherever possible," starting in 2018.[12]

Despite no apparent unauthorized trades or transfers in customers' accounts resulting from these email account compromises, the SEC still found that the "Cetera Entities violated the Safeguards Rule because their policies and procedures to protect customer information and to prevent and respond to cybersecurity incidents were not reasonably designed to meet these objectives."[13] In particular, the SEC noted that the Cetera Entities had "a significant number of security tools at their disposal that

allowed them to implement controls that would mitigate these higher risks," but that these tools were not utilized "in the manner tailored to their business, exposing their customers' PII to unreasonable risks."[14]

In addition to the Safeguards Rule violations, the SEC also found that Cetera Advisors LLC and Cetera Investment Advisers LLC violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder "by failing to adopt and implement reasonably designed policies and procedures regarding review of communications to advisory clients," which resulted in misleading breach notifications to clients.[15] Specifically, the SEC found that some breach notifications sent by the Cetera Entities in 2018 to approximately 220 advisory clients used template language calling the email account intrusions "recent" and stating the breaches were discovered two months before these notification letters, when the breaches had actually been discovered "at least six months earlier."[16]

The Cetera Entities will pay a $300,000 penalty as a result of this settlement.

CAMBRIDGE

In the action against Cambridge, the SEC found that, from January 2018 to July 1, 2021, cloud-based email accounts for over 121 of Cambridge's independent contractors were compromised, resulting in the potential access or exfiltration of approximately 5,977 customers' PII.[17]

The SEC specifically noted that Cambridge violated the Safeguards Rule because, even though it learned of the first "email account takeover in January 2018, it failed to adopt and implement firm wide enhanced security measures for cloud-based email accounts of its independent representatives in its written policies and procedures, such as the use of [MFA] for all Cambridge users until 2021."[18] According to the SEC, this lack of action by Cambridge potentially resulted in additional exposure of PII. As with the Cetera Entities, the SEC noted that there were no apparent unauthorized trades or fund transfers out of Cambridge customer accounts that resulted from these intrusions.

Cambridge will pay a $250,000 penalty as a result of this settlement.

KMS

The third action announced by the SEC on August 30, 2021, was directed at KMS, which is both a registered broker-dealer and investment adviser. The SEC found that between September 2018 and December 2019, 15 KMS financial adviser email accounts were compromised, resulting in the exposure of customer records and information, including PII of approximately 4,900 customers.[19]

The SEC found that "KMS's incident response policy was not reasonably designed to ensure that the email account compromises were remediated in a timely manner to ensure the protection of customer PII" and that, "[a]lthough KMS discovered the first email account compromise in November 2018, it failed to adopt written policies and procedures requiring additional firm-wide security measures for all KMS email users until May 2020, and did not fully implement those measures until August 2020."[20] As with the Cetera Entities and Cambridge actions, the SEC noted that the email account intrusions "do not appear to have resulted in any unauthorized trades or fund transfers to unauthorized parties for any KMS customer accounts."[21]

KMS will pay a $200,000 penalty as a result of this settlement.

The Pearson Settlement

The above actions followed on the heels of the SEC's settlement with Pearson that allegedly violated its obligations related to cybersecurity disclosures for public companies. Public companies not only have a responsibility to disclose material information to investors in SEC filings, they also must maintain disclosure controls and procedures designed to ensure that such material information "is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms."[22]

According to the SEC's order, Pearson originally learned in March 2019 that millions of rows of data stored on its system's server had been accessed and downloaded by a "sophisticated threat actor" who had discovered an unpatched vulnerability on the server.[23] A software manufacturer flagged the server vulnerability in September 2018, but Pearson declined to implement the available patch until after it learned of the breach.[24]

Pearson organized an incident management response team and retained a third-party consultant to investigate the breach. After completing its review of the incident, Pearson mailed a breach notice on July 19, 2019, to the approximately 13,000 customer accounts affected by the intrusion. However, the notice failed to inform school administrators that their usernames and passwords had been exfiltrated, such that "the impacted accounts continued to be at risk after July 19, 2019."[25]

The SEC charges stem from Pearson's statements to investors following these actions. First, Pearson's July 2019 semi-annual report on Form 6-K filed with the SEC contained a risk factor disclosure describing a *hypothetical* risk of a data breach. In this report's "[p]rincipal risks and uncertainties" section, Pearson stated that a "[r]isk of a data privacy incident or other failure to comply with data privacy regulations and standards and/or a weakness in information security, including a failure to prevent or detect a malicious attack on our systems, could result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss."[26] This disclosure, which also appeared in Pearson's prior reports on Form 6-K, was not updated, implying that no "major data privacy or confidentiality breach" had occurred during the relevant period—despite the fact that Pearson learned of the data breach in March 2019 and sent breach notices to affected customers in July 2019.[27]

In addition to Pearson's disclosure in its SEC filing, the SEC's order also highlights statements made by Pearson to the media in July 2019 as containing material misstatements and omissions. For example:

- Although Pearson knew that millions of rows of data had been exfiltrated from the breached server, Pearson described the incident merely as "unauthorized access" and "expos[ure of] data."
- Pearson stated that the breach "in some instances may" have included dates of birth and/or email addresses, when, in fact, Pearson knew that almost half of the compromised data included dates of birth, and that a significant portion included email addresses.
- Pearson stated that it had "strict data protections in place," when, in fact, Pearson failed to patch a critical server vulnerability for six months and used an outdated hashing algorithm for password storage.
- Pearson also omitted the fact that millions of rows of student data and login information was stolen.

Following Pearson's public misstatements about the data breach, Pearson continued to offer its ordinary shares under the company's employee and management incentive plans.[28] The SEC's order emphasizes that although protecting customer data was critical to Pearson's business, and that Pearson had identified the risk for unauthorized access to this data as significant, Pearson failed to "maintain disclosure controls and procedures designed to analyze or assess such incidents for potential disclosure in the company's filings."[29] The SEC's order found Pearson violated sections of the Securities Act of 1933 and the Securities Exchange Act of 1934 ("Exchange Act") and rules promulgated thereunder.[30] Without admitting or denying the SEC's findings, Pearson agreed to a cease-and-desist order requiring the company not to engage in violations of federal securities laws, and to pay a $1 million civil penalty.

Takeaways for SEC Registrants

The increase in cyber-related SEC enforcement actions comes as no big surprise. The SEC Enforcement Division's Cyber Unit was established in 2017 to increase the agency's focus on cyber-related misconduct.[31] SEC registrants should look to these enforcement actions as instructive for their own disclosure and cybersecurity programs. Below are some key points to consider as companies develop and augment their internal compliance programs to ensure they are properly prepared for increased SEC scrutiny on cybersecurity issues.

For all SEC registrants: Cybersecurity breaches are an increasing risk, and registrants need to be aware of what SEC rules are implicated when a breach occurs. Review your current cybersecurity policies and procedures to ensure they account for your obligations under SEC rules. Then be sure to actually implement and follow the procedures set forth in the policies.

For public reporting companies: Public companies have been on notice for some time that the SEC expects timely and accurate disclosure with respect to cybersecurity risks and events. Following the creation of the Enforcement Division's Cyber Unit, the SEC published interpretive guidance in 2018, which reinforced and expanded on earlier guidance issued by the SEC staff. The 2018 SEC guidance explained that, despite the fact that there are no prescriptive disclosure requirements related to cybersecurity risks and incidents, companies may still have disclosure obligations, and should have disclosure controls and procedures in place to ensure that investors receive material information. Public companies should view the Pearson settlement as a reminder that disclosure controls and procedures must include clear instructions on how to identify and elevate information around security incidents to executive officers so that appropriate disclosures can be made in SEC filings, as well as in other public statements. Risk factors with hypothetical language will not suffice if the risk is no longer hypothetical. As such, companies should regularly review risk factor disclosure to ensure accuracy and update language to the extent necessary. Public statements made outside of SEC filings will also be scrutinized by the SEC. Following data breaches, companies should carefully coordinate their public relations, communications and legal strategies. Now is a good time to revisit the SEC's 2018 guidance.

For registered entities: The actions announced last month demonstrate that cybersecurity is a perennial top priority in SEC examinations, as recently reiterated in the Division of Examination's 2021 examination priorities.[32] Furthermore, these actions underscore the importance that registered entities continue to review any gaps in cybersecurity policies and procedures for possible improvements, and ensure that business practices, testing and implementation align with written policies and applicable law.

Looking forward: In addition to the recent uptick in enforcement of current SEC rules, it is expected that the SEC may soon propose new rules on cybersecurity applicable to both public companies and investment funds. SEC Chair Gensler testified in front of Congress on September 14, 2021, that he had directed SEC staff to consider recommending public company disclosure requirements around cyber hygiene, incident reporting and cybersecurity expertise on the board of directors.[33] Chair Gensler also indicated that he has directed the staff to look at cybersecurity implications for investment management. It will be important to follow legislative developments and any related SEC guidance on this issue over the coming months.

Anjani Nadadur, Joshua Silverstein and Julie Sweeney contributed to this Legal Update.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Richard M. Rosenfeld
+1 202 263 3130
rrosenfeld@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Christina M. Thomas
+1 202 263 3344
cmthomas@mayerbrown.com

Endnotes

[1] SEC Press Release, SEC Division of Examinations Announces 2021 Examination Priorities (March 3, 2021), *available at* https://www.sec.gov/news/press-release/2021-39.

[2] *See* SEC Statement and Guidance on Public Company Cybersecurity Disclosures, Rel. Nos. 33-10459, 34-82746 (Feb. 26, 2018) (*codified at* 17 C.F.R. §§ 229 and 249), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[3] *See* SEC Press Release, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (August 30, 2021), *available at* SEC.gov | SEC Announces Three Actions Charging Deficient Cybersecurity Procedures.

[4] *See id.*

[5] *See* SEC Press Release, SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Aug. 16, 2021), *available at* SEC.gov | SEC Charges Pearson plc for Misleading Investors About Cyber Breach.

[6] 15 U.S.C. §§6801 et seq.

[7] *Privacy of Consumer Financial Information (Regulation S-P)*, Rel. Nos. 34-42974, IA-1883, 65 Fed. Reg. 40,334 (June 29, 2000) (*codified at* 17 C.F.R. §§ 248.1-248.30).

[8] *Disposal of Consumer Report Information*, Rel. Nos. 34-50781, IA-2332, IC-26685, 69 Fed. Reg. 71,329 (Dec. 8, 2004) (*codified at* 17 C.F.R. § 248.30(b)).

[9] *See* SEC Press Release, *supra* note 3.

[10] *See id.*

[11] *In the Matter of Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, Cetera Advisors LLC, and Cetera Investment Advisers LLC*, Rel. Nos. 34-92,800, IA- 5,834 (Aug. 30, 2021), *available at* Cetera Advisor Networks LLC, et al. (sec.gov).

[12] Cetera Order, *supra* note 12.

[13] *Id*.

[14] *Id*.

[15] *Id*.

[16] *Id*.

[17] *In the Matter of Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc.*, Rel. Nos. 34-92,806, IA-5,839 (Aug. 30, 2021), *available at* Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc. (sec.gov).

[18] *See id*.

[19] *In the Matter of KMS Financial Services, Inc.*, Rel. Nos. 34-92,807, IA-5,840 (Aug. 30, 2021), *available at* KMS Financial Services, Inc. (sec.gov).

[20] *Id*.

[21] *Id*.

[22] 17 C.F.R. § 240.13a-15 (Exchange Act Rule 13a-15(a)).

[23] *In the Matter of Pearson plc*, Rel. Nos. 33-10,963, 34-92,676 (Aug. 16, 2021), *available at* Pearson Plc (sec.gov).

[24] *Id*.

[25] *Id*.

[26] *Id*.

[27] *Id*.

[28] *Id*.

[29] *Id*.

[30] The SEC specifically found that Pearson violated Sections 17(a)(2) and 17(a)(3) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-15(a), and 13a-16 thereunder.

[31] *See* SEC Press Release, SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors (Sept. 25, 2017), *available at* https://www.sec.gov/news/press-release/2017-176.

[32] *See* the SEC's 2021 Spring Annual Regulatory Agenda, *available at* https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=7CE97CC2D49C9B6B70868F7B2752E582C86F1945A4A46F34426C18AF1ABE101E611318F64B67159C3A36E7556BD0FB872C8F.

[33] *Oversight of the US Securities and Exchange Commission*, 117th Cong. (2021) (testimony of the Honorable Gary Gensler), *available at* https://www.banking.senate.gov/hearings/09/10/2021/oversight-of-the-us-securities-and-exchange-commission.