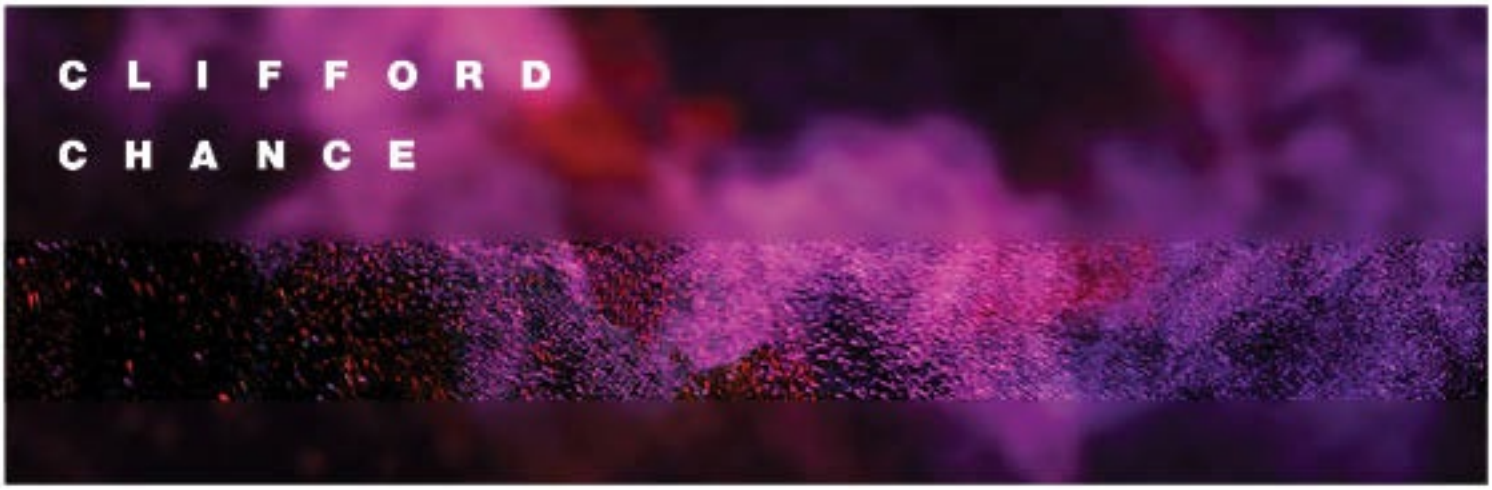

SEC FINES EIGHT FIRMS FOR DEFICIENT CYBERSECURITY PRACTICES, ISSUES WARNING ABOUT IMPORTANCE OF ROBUST POLICIES AND PROCEDURES AND ACCURATE DISCLOSURES

In a strong statement about the importance of cybersecurity controls, on August 30, 2021, the Securities and Exchange Commission ("SEC" or "Commission") announced fines against eight registered investment advisers and broker-dealers for deficient cybersecurity practices that led to breaches of personal information of thousands of clients and customers. The charges come just days after the agency announced a $1,000,000 fine against a London-based publisher for improper disclosures relating to a 2018 cybersecurity breach,[1] a clear indication that the Commission will continue its focus on ensuring registered entities have adequate measures in place to protect the personal data of their clients and customers. Emphasizing that the Commission expects more than just policies that appear appropriate on paper, Cyber Unit Chief Kristina Littman warned that it was "not enough to write a policy" if those policies aren't fully implemented.[2] Notably, each charge highlighted the failure to require multi-factor authentication ("MFA") for email accounts of independent contractors with access to client and customer data—a strong signal to the industry to implement these security measures.

Key issues

- The SEC fined eight firms for deficient cybersecurity practices related to takeovers of independent contractor email accounts with access to sensitive client and customer data.
- The SEC took issue with the failure of these companies to effectively implement their written policies and procedures.
- Several of the firms also failed to effectively review breach notifications that contained misleading information.
- Registered investment advisers and broker-dealers should take this opportunity to review their policies and procedures to ensure that they are fully implemented and reflect updated risks and vulnerabilities.
- In particular, firms should consider implementing multi-factor authentication for email accounts, especially for independent contractors.

SAFEGUARDS RULE AND DISCLOSURE REQUIREMENTS

Regulation S-P was enacted by the SEC in 2000 to implement the privacy provisions of the Gramm-Leach-Bliley Act ("GLBA"). One of the rules

---

1 For more on this enforcement action, see our briefing here.

2 Press Release, *SEC Announces Three Actions Charging Deficient Cybersecurity Procedures* (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169.

implemented as part of Regulation S-P is the Safeguards Rule, Rule 30(a), which requires all investment advisers and broker-dealers registered with the Commission to adopt policies and procedures that are reasonably designed to safeguard the security and confidentiality of customer personal information, protect this information against anticipated threats, and prevent unauthorized access and use of this information in any manner that could result in substantial harm or inconvenience to any customer.

In addition, Section 206(4) of the Investment Advisers Act of 1940 and Rule 206(4)-7 require registered advisers to implement compliance policies and procedures to ensure that communications to clients are reviewed to avoid misleading or inaccurate information.[3]

BACKGROUND: DEFICIENT POLICIES AND PROCEDURES

Each of the eight charged firms suffered data breaches as a result of email account takeovers that the Commission alleged could have been prevented with "reasonably designed" policies and procedures to safeguard client and customer records and information.

Cetera Financial Group, Inc.

The first Commission order found that five subsidiaries of Cetera Financial Group, Inc. (the "Cetera Entities") failed to implement MFA for email accounts of independent contractors that contained client and customer personal data, despite repeated email account takeovers and a policy mandating MFA. According to the order, the Cetera Entities first began experiencing email account takeovers in November 2017, when 32 accounts containing client and customer personal data were taken over via phishing and other similar attacks. Following the attacks, the SEC found that the Cetera Entities began implementing MFA for email accounts and revised their policies to require MFA "wherever possible" and "at a minimum for privileged or high-risk access." However, the rollout was incomplete, and in particular, many of the email accounts of representatives and offshore contractors remained unprotected. The SEC order identified 67 accounts in total that had been taken over, resulting in the exposure of the personal data of thousands of clients and customers. All of the accounts were unprotected, in that they did not use MFA. The SEC order concluded that the Cetera Entities' MFA policy was not "reasonably designed" to apply to the email accounts of the representatives and offshore contractors, despite the fact that these accounts had access to sensitive client and customer data.

The SEC also found fault with the breach notifications that the Cetera Entities sent to clients and customers whose personal data was compromised. Whenever a Cetera Entity determined that client and customer data was compromised, it sent a breach notification to the affected clients and customers, generally with the assistance of outside counsel. Upon review, the Commission determined that approximately 220 of these notifications included template language that was inaccurate and misleading. Specifically, the notifications stated that the incidents were "recent" and discovered two months before the notification, when in fact, according to the SEC, the Cetera Entities had learned of the respective breaches at least six months earlier. The Commission faulted the Cetera Entities with failing

[3] Also see our briefing here for other SEC rules on making required disclosures.

to correct the misleading language despite policies in place requiring Cetera personnel to review client communications before they were issued.

The Cetera Entities neither admitted nor denied the Commission's charges, but agreed to be censured, to cease and desist from further violations, and to collectively pay $300,000 in fines. The SEC order also acknowledged that the Cetera Entities had implemented remedial acts, which the SEC considered in determining the penalty.

Cambridge Investment Research

The SEC also found that Cambridge Investment Research, Inc., and Cambridge Investment Research Advisors, Inc. (the "Cambridge Entities") failed to implement enhanced security measures despite determining numerous email accounts of independent representatives had been compromised from 2017 through 2021. According to the Commission's order, following each email account takeover, the Cambridge Entities suspended the affected independent representative's account and reset the account password. The Cambridge Entities also "recommended" that the independent representatives implement enhanced security measures, such as MFA, but only some representatives did so. The Cambridge Entities continued to encounter email account takeovers of independent representatives with access to customer and client personal data. Only in April of 2021 did the Cambridge Entities revise their policies to require MFA for all cloud-based email accounts.

The Cambridge Entities neither admitted nor denied the Commission's charges, but agreed to be censured, to cease and desist from further violations, and to collectively pay $250,000 in fines. The SEC order also acknowledged that the Cambridge Entities had implemented remedial acts, which the SEC considered in determining the penalty.

KMS Financial Services, Inc.

The final SEC order charged KMS Financial Services, Inc. ("KMS") with failing to adopt written policies and procedures reasonably designed to safeguard client and customer records and information accessible through its cloud-based email system. Between 2018 and 2020, fifteen independent financial advisers associated with KMS experienced email account takeovers, leading to the exposure of personal data of approximately 4,900 KMS clients and customers. After the first attack was uncovered, KMS began implementing enhanced security measures, including MFA. It also hired forensic firms to investigate and issue incident reports, several of which recommended enabling MFA as a remedial measure. However, according to the SEC, KMS did not require enhanced security measures (including MFA) until May 2020—and it did not fully implement additional security measures (including MFA) until August 2020.

KMS neither admitted nor denied the Commission's charges, but agreed to be censured, to cease and desist from further violations, and to pay $200,000 in fines. The SEC order also acknowledged that KMS had implemented remedial acts, which the SEC considered in determining the penalty.

CONCLUSION

Ever since the SEC issued its first fine for violations of Regulation S-P ten years ago in 2011,[4] the SEC has increasingly focused on cybersecurity enforcement. In 2015, the Office of Compliance Inspections and Examinations ("OCIE") announced a cybersecurity exam initiative, and in 2017 the agency created its Cyber Unit. Then in early 2019 OCIE announced another cybersecurity sweep, followed shortly thereafter with a risk alert highlighting key regulation S-P deficiencies and non-compliance issues that the agency had observed during its examinations.[5] These OCIE examinations now appear to have led to the first—but certainly not the last—set of penalties for noncompliance, with the agency's press release notably thanking examination teams from Chicago and New York, along with a host of OCIE staff.

The implication for registered investment advisers and broker-dealers is clear: paper policies alone are not sufficient, particularly if there is evidence of past cybersecurity incidents. Rather, the Commission expects companies to timely and effectively implement written policies and procedures. And while the Safeguards Rule does not mandate that firms implement specific cybersecurity measures, companies are on notice to regularly update and review implementation of their policies and procedures to take into consideration updated risks, historic vulnerabilities, and evolving industry standards. In particular, these newest actions suggest that the SEC considers multi-factor authentication to be a key security measure for cloud-based email accounts that have access to client and customer data—especially for independent contractors. Companies would be well-advised to consider implementing such measures, whether or not they have suffered breaches in the past.

Good cyber hygiene and risk management starts long before an incident occurs. Clifford Chance has published a number of reports and briefings to help companies protect themselves from attacks and vulnerabilities. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook.

4 See *In the Matter of Frederick O. Kraus*, SEC No. 64221 (Apr. 7, 2011).
5 For more on the risk alert, see our client briefing here.

CONTACTS

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Megan Gordon
Managing Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com