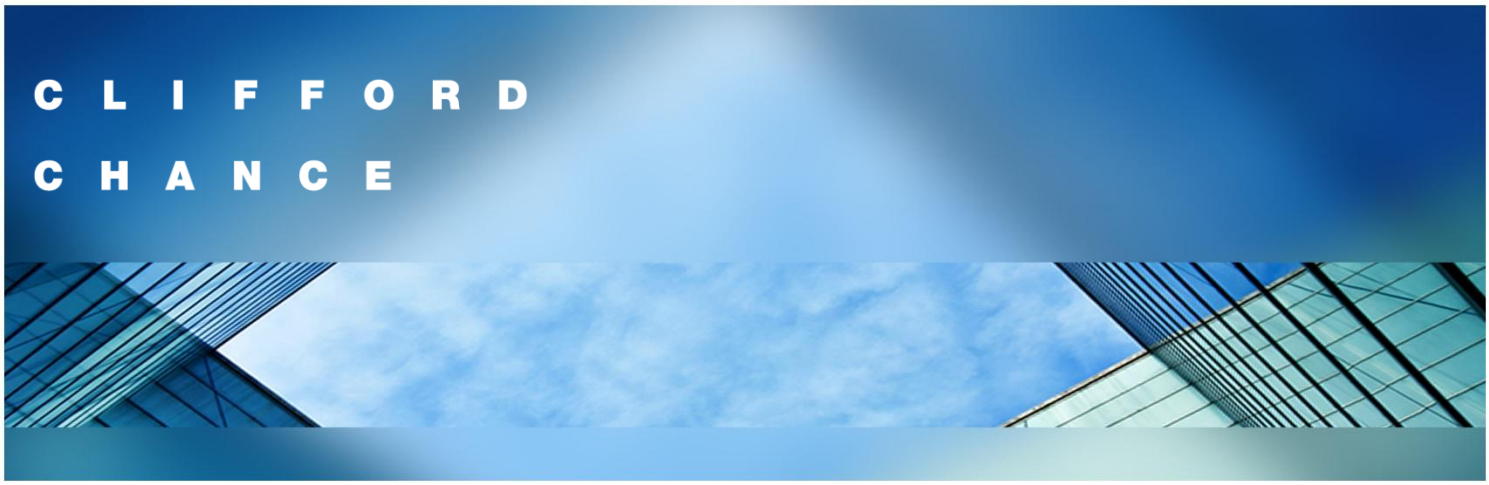


EQUIFAX HACK, SEC DATA BREACH BRING ISSUER DISCLOSURE OBLIGATIONS TO THE FOREFRONT

The recent Equifax data breach focuses attention on the necessity of adequate disclosure by public companies of material cybersecurity-related events. Both SEC Chair Jay Clayton and Stephanie Avakian, the Co-Director of the Division of Enforcement, have made clear that they would "like to see better disclosure around [cybersecurity]"[i] and could "absolutely" bring a cybersecurity disclosure enforcement action.[ii] In addition, the SEC's recent disclosures of its own breach will likely increase focus within the agency on its external enforcement efforts.

THE SEC'S CYBERSECURITY EFFORTS

The SEC has had the authority to regulate cybersecurity at broker-dealers and other registered-entities since at least 2000, when it promulgated Regulation S-P.[iii] This regulation requires financial institutions to adopt policies that are reasonably designed to safeguard customers' nonpublic personal information, protect that information against anticipated threats, and prevent unauthorized access and use of nonpublic material information that could result in significant harm to the customer. Nonetheless, the SEC was initially slow to use this authority, bringing its first cybersecurity enforcement action in 2015.

In the 2015 case, *In re R.T. Jones Capital Equities Management, Inc.*,[iv] the SEC alleged that R.T. Jones stored sensitive personally identifiable information ("PII") of clients and others on a third party-hosted web server. In July 2013, the server was hacked, rendering the PII of more than 100,000 individuals vulnerable to theft. After *R.T. Jones,* the SEC subsequently brought a similar case in 2016 against a registered investment adviser.[v]

The SEC has made cybersecurity a focus of its annual Office of Compliance Inspections and Examinations ("OCIE") cycle of examinations of registered investment advisers since January 2014. In that initial 2014 examination cycle, OCIE asked firms for information on their identification of cyber risks; the protection of the firm's network; the risks associated with customer, vendor and other third-party access; the detection of unauthorized activity; and whether the firm had suffered a cyber incident and how it responded to that incident. This was in turn followed by the Cybersecurity 2 initiative in January 2015, which built on the initial 2014 exam, but also involved validation and testing of procedures and controls surrounding cybersecurity preparedness.

The SEC has also taken steps to regulate issuer cybersecurity. In October 2011, the Division of Corporation Finance issued cybersecurity guidance. The SEC's guidance reflects the SEC staff's opinion as to how disclosure of cybersecurity risks and incidents should be treated under current securities laws.[vi] It advises that disclosure of cybersecurity risks may be necessary for a company to fulfill its existing obligation to disclose information that a "reasonable investor would consider important to an investment decision."[vii] "[C]osts or other consequences" of a cyber breach, such as costs of remediation and protection measures, lost revenues, reputational damage, and litigation risk, may need to be disclosed to the extent they are "reasonably likely to have a material effect on the registrant's results."[viii] Risks of cyber incidents should be disclosed among a company's "Risk Factors;" specific material cybersecurity breaches should be

disclosed under the "Management's Discussion and Analysis" heading.[ix]

Thus far, relatively few companies have disclosed cybersecurity breaches, in part because, as the guidance acknowledges, companies are not expected to disclose details that would compromise their cybersecurity efforts.[x] Nonetheless, the SEC has directed companies to disclose information on specific cyber attacks in comment letters — the form of the agency's response to requests for comment on its rules and other communications. Amazon, for example, was compelled to disclose details of attacks suffered by its subsidiaries.[xi] Indeed, the agency has surpassed its own guidance, apparently requiring disclosure of even non-material cyber attacks or, in the language of one comment letter, "any" cyber attack that the company had suffered.[xii]

THE EQUIFAX HACK

Equifax has reported that it learned on July 29, 2017 that in May 2017 hackers gained access to its system and stole PII, including Social Security numbers, license numbers, addresses, and birth dates for approximately 143 million people, as well as over 200,000 credit card numbers. Since announcing the breach on September 7, 2017, Equifax has lost $4 billion in market value and faces multiple lawsuits, investigations by state and federal authorities and Congressional investigations. However, it appears that Equifax did not have any pre-hack disclosures regarding cybersecurity risk and made its post-hack disclosure over a month after the breach was discovered.

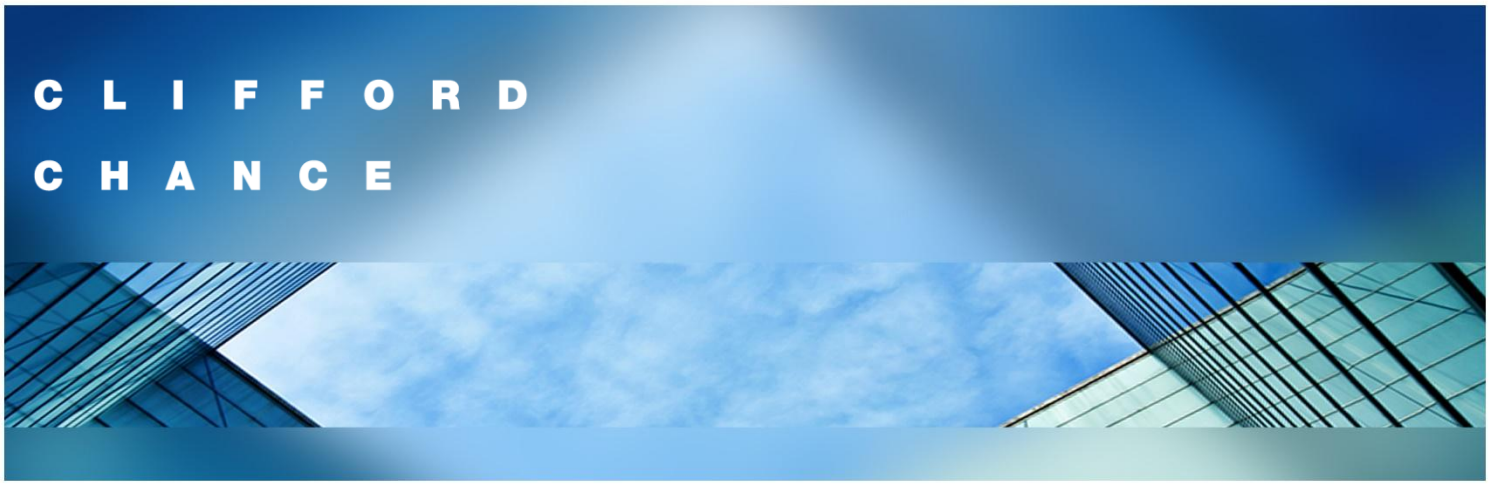
These decisions are likely to be subject to significant scrutiny from the SEC, which will want to understand whether Equifax was aware of material cybersecurity risks before the breach, how and when Equifax investigated the breach, and the factors that influenced the timing of the disclosure. Conceivably, the SEC could seek to bring an action alleging that Equifax's failure to adequately disclose its cyber risk constituted a violation. Or, the SEC could seek to establish a books and records violation, supported by the SEC's statement in its cybersecurity guidance that breaches may require recognition of impaired assets and reductions in projected future cash flows.

The timing of Equifax's post-hack disclosure may also be an area of interest for the SEC, although it would likely be difficult for the SEC to allege a securities law violation based on Equifax's apparent delay in disclosing the hack. Equifax disclosed the breach to the market through a Form 8-K filing, which is the filing that a corporation uses to disclose significant corporate events. Equifax's Form 8-K disclosed the hack as an "Item 8.01" disclosure, which is used for voluntary disclosures of material events. Because the hack was disclosed as an Item 8.01 event, Equifax did not have to make the disclosure within a set time period. Nonetheless, given the significant market impact of the breach, the SEC is likely to carefully analyze whether this Item 8.01 disclosure was appropriate or if, instead, Equifax should have filed the Form 8-K as an Item 2.06 material impairment. In addition, any indication that Equifax purposefully delayed making the breach disclosure to affect share price could give rise to a securities fraud investigation.

Finally, reports indicate that Equifax will also face scrutiny regarding sales of securities by senior executives in the days following the discovery of the breach.

CONCLUSION

To date, the SEC has not yet brought a disclosure-based cybersecurity enforcement action. However, the SEC's recent announcement that it suffered a major breach of the EDGAR system, which was announced in conjunction with Chair Clayton's statements regarding the Commission's focus on external cybersecurity efforts, may make the SEC inclined to take a more aggressive approach to cybersecurity enforcement. This approach was explicitly foreshadowed by the SEC's announcement of the EDGAR breach, which noted that "[i]ssuers and other market participants must take their periodic and current disclosure obligations regarding cybersecurity risks seriously, and failure to do so may result in an enforcement action."[xiii] Companies must continually reassess their cybersecurity preparedness to ensure that they have a comprehensive response plan in place, which includes consideration of the relevant disclosure requirements.



CONTACTS

Megan Gordon
Partner

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

Daniel Silver
Partner

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

Benjamin Berringer
Associate

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

---

i Carmen Germaine, *Clayton Says No Shift in Enforcement Priorities at SEC*, Law360 (Sept. 6, 2017), https://www.law360.com/articles/961063/clayton-says-no-shift-in-enforcement-priorities-at-sec.

ii Jimmy Hoover, *SEC Suits Over Cyber Reporting Could Be On Horizon*, Law360 (Apr. 20, 2017), https://www.law360.com/articles/915377/sec-suits-over-cyber-reporting-could-be-on-horizon.

iii Regulation S-P, 17 C.F.R. 248.30 (2017).

iv 112 S.E.C. Docket 2848 (Sept. 22, 2015).

v *In re Morgan Staley Smith Barney LLC*, S.E.C. Release No. 4415 (June 8, 2016).

vi Securities and Exchange Commission, *CF Disclosure Guidance, Topic No. 2: Cybersecurity* (Oct. 13, 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

vii *Id.*

viii *Id.*

ix *Id.*

x *Id.*

xi Amazon.com, Inc., SEC Comment Letter (April 18, 2012).

xii *See, e.g.*, Hilton Worldwide Inc., SEC Comment Letter (Oct. 13, 2013) ("If you have experienced any cyber attacks in the past, please state that fact in any additional risk factor disclosure in order to provide the proper context."); Freeport-McMoRan Copper & Gold Inc., SEC Comment Letter (July 16, 2012) (same); Apache Corporation, SEC Comment Letter (July 16, 2012) (same); Valero Energy Corporation, SEC Comment Letter (May 18, 2012) (same); Quintiles Transnational Holdings Inc., SEC Comment Letter (Apr. 16, 2013) (instructed to revise disclosure to include "any security breaches, cyber attacks or other similar events"); ConocoPhillips, SEC Comment Letter (Sept. 26, 2012) (requesting that a revised risk factor state that the company has "experienced occasional actual and attempted breaches of [its] cybersecurity"); Equifax, Inc., SEC Comment Letter (Sept. 7, 2012) (requesting that corporation disclose any historical cyber attacks in future filings); Anheuser-Busch Inbev SA NV, SEC Comment Letter (Aug. 17, 2012) (same).

xiii Jay Clayton, Chairman, Sec. Exch. Comm'n, Statement on Cybersecurity (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20.