ALERT MEMORANDUM

Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide

June 5, 2018

If you have any questions concerning this memorandum, please reach out to your regular firm contact or any of our partners and counsel listed under Cybersecurity and Privacy and Capital Markets in the "Our Practice" section of our website.

NEW YORK
One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999

The consequences of a cybersecurity incident can be severe. The economic loss associated with an incident can often be compounded by reputational damage, loss of trade secrets, destruction of assets, operational impairment, lost revenue following the announcement of the cybersecurity incident and the expense of implementing remedial measures. The timing and content of any public communication about a suspected or confirmed cybersecurity incident can exacerbate this loss and have a significant impact on the trading price of the issuer's securities.[1] The disclosure considerations become even more complex when a company is subject to overlapping, and potentially conflicting, regulatory obligations in multiple jurisdictions, including the United States and the European Union ("EU"). This issue is now at the forefront with the EU's new data security and privacy regime, the General Data Protection Regulation ("GDPR"), which became effective on May 25, 2018.

Regulators are taking notice. In the United States, prosecutors and other enforcement authorities have begun scrutinizing the timing of public disclosures relating to cybersecurity incidents. For example, Altaba, formerly known as Yahoo, recently entered into a settlement with the Securities and Exchange Commission ("SEC" or the "Commission") to resolve allegations that Yahoo violated federal securities laws in connection with the disclosure of the 2014 cybersecurity incident involving its user database.[2] The U.S. Department of Justice ("DOJ") and SEC have also filed charges for alleged insider trading in violation of federal securities laws against a former Equifax executive who is alleged to have traded in Equifax securities while in possession of material information concerning a cybersecurity incident that was at the time not yet known to the public.[3]

[1] For example, Facebook's share price fell by almost 7% on March 19, 2018 (the biggest one-day drop in Facebook's share price since March 2014) in connection with the public disclosure of Cambridge Analytica's apparent unauthorized access to personal data of about 50 million Facebook users (this estimate was subsequently revised to 87 million Facebook users).

[2] This case represents the first time a public company has been charged by the SEC for failing to adequately disclose a cybersecurity incident. For a more detailed discussion, see our prior alert memorandum: https://www.clearygottlieb.com/news-and-insights/publication-listing/yahoos-successor-settles-first-ever-case-involving-sec-charges-for-failing.

[3] For a more detailed discussion, see our prior blog post: https://www.clearycyberwatch.com/2018/03/doj-sec-charge-former-equifax-executive-insider-trading/.

In the United States, the disclosure obligations for public companies are governed by the federal securities laws and the SEC rules promulgated thereunder. In the context of cybersecurity incidents, these disclosure obligations often intersect with U.S. state law and other U.S. and non-U.S. legal obligations that may require disclosure of incidents to affected customers.

In the EU, companies must comply with the Market Abuse Regulation ("MAR") and its implementing legislation as well as data protection rules primarily regulated by GDPR. MAR generally applies to U.S. companies with debt, equity or other securities admitted to trading on EU-regulated markets or multilateral trading facilities (or for which a request for admission to trading has been made) or companies with securities traded on an EU-organized trading facility. GDPR applies to U.S. companies with an operational or jurisdictional presence in the EU.[4]

In this memorandum, we provide an overview of the key U.S. and EU legal regimes concerning the disclosure of cybersecurity incidents from the perspective of a U.S. company subject to the disclosure requirements of multiple jurisdictions.

Understanding U.S. Disclosure Requirements

In the absence of a specific duty to disclose, the U.S. federal securities laws do not generally require reporting issuers to publicly disclose all material developments as soon as they occur.[5] Although the SEC and the rules of the U.S. securities exchanges encourage prompt disclosure of material information, the precise timing of many important corporate disclosures, including those relating to cybersecurity incidents, often allows for the exercise of judgment by corporate officials.

While disclosure requirements under the U.S. Securities Act of 1933 (the "Securities Act") and the U.S. Securities Exchange Act of 1934 (the "Exchange Act") do not specifically address the disclosure of cybersecurity risks and incidents, a number of the existing disclosure requirements of the Securities Act and the Exchange Act may impose an obligation for issuers to disclose cyber-related matters when they are making required annual or quarterly disclosures or in connection with the offering of securities. The determination of whether a company must make such disclosures is based on generally applicable standards of materiality. The U.S. Supreme Court has held that information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it "would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available" to the shareholder.[6] Additionally, a company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."[7] In an effort to assist public companies when considering, drafting and issuing disclosure about cybersecurity risks and incidents, the Division of Corporation Finance in 2011, and then the Commission in 2018, each published cybersecurity guidance.

[4] For a more detailed discussion on the interplay between MAR and GDPR, see our prior alert memorandum: https://www.clearygottlieb.com/-/media/files/alert-memos-2018/eu-regulated-companies-faced-with-personal-data-breach--reconciling-obligations-under-gdpr--mar.pdf.

[5] Periodic reports, such as Forms 10-K and 10-Q, call for disclosure of specified information on a periodic basis, and domestic issuers are required to report certain types of events on Form 8-K soon after they occur. But in the absence of a specific duty to disclose, the U.S. federal securities laws do not require issuers to make immediate public disclosure of material information so long as they (and their insiders) abstain from transactions in their own securities and comply with Regulation FD (as discussed below).

[6] *TSC Industries v. Northway*, 426 U.S. 438, 449 (1976); *Basic Inc. v. Levinson*, 485 U.S. 224, 231-32 (1988) (internal citation omitted).

[7] 17 CFR § 408; 17 CFR § 240.12b-20; 17 CFR § 240.14a-9.

SEC Cybersecurity Guidance

The disclosure guidance issued by the Division of Corporation Finance in 2011 (the "2011 Division guidance") did not impose any new disclosure obligations on public companies, but rather identified cybersecurity as a business risk that, like other operational and financial risks, may call for disclosure if it could materially impact a company's operations. The Commission's 2018 interpretive release on cybersecurity disclosure (the "2018 interpretive guidance") reaffirms the 2011 Division guidance in this respect.

The 2018 interpretive guidance addresses the areas of disclosure that had been the focus of the 2011 Division guidance and expands upon the considerations that companies should review when determining whether disclosure is required and, if so, the scope of such disclosure. As was the case in the 2011 Division guidance, the 2018 interpretive guidance reminds companies to consider cybersecurity disclosure in the context of risk factors, management's discussion and analysis of financial condition and results of operations, business description, legal proceedings and financial statement disclosure. In addition, the 2018 interpretive guidance also reminds companies that, to the extent cybersecurity risks are material to a company's business, companies should disclose how the board oversees the management of such risk in their proxy statement as required by Item 407(h) of Regulation S-K.

The 2018 interpretive guidance suggests that, in determining their disclosure obligations, companies should weigh "the importance of any compromised information and the impact of the incident on the company's operations." The guidance adds that the materiality of cybersecurity risks and incidents depends "upon their nature, extent and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations."[8] The 2018 interpretive guidance highlights a number of factors that may inform the materiality determination, including the range of harm that cybersecurity incidents could have on a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.

When disclosure is required, the Commission expects companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents, including as it relates to "the concomitant financial, legal and reputational consequences," and placed in the appropriate context. In this regard, the 2018 interpretive guidance reiterates the need for non-generic cyber-related disclosure, though specific technical information is not required if it would compromise a company's cybersecurity protections and any remedial efforts.

In addition, while an ongoing internal or external investigation of a material cybersecurity incident does not on its own provide a basis for avoiding disclosure, the Commission is mindful that some material facts may not be available at the time of the initial disclosure. Therefore, the 2018 interpretive guidance reminds companies that they may have a duty to correct prior disclosure that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made or a duty to update disclosure that becomes materially inaccurate after it is made.[9]

[8] For a more detailed discussion of the 2018 interpretive guidance, see our prior alert memorandum: https://www.clearygottlieb.com/news-and-insights/publication-listing/sec-issues-interpretive-release-on-cybersecurity-disclosure.

[9] The federal securities laws do not impose a general affirmative duty on public companies to continuously disclose material information and, as acknowledged in Footnote 37 of the 2018 interpretive guidance, circuits are split on whether a duty to update exists. However, in circuits where a duty to update has been found to exist, a distinction has often been drawn between statements of a policy nature that are within the company's control and statements describing then current facts that would be expected to change over time. The former have been held subject to a duty to update while the latter have not. *See In re Advanta Corp. Securities Litigation*, 180 F.3d 525, 536 (3d Cir. 1997) ("[T]he voluntary disclosure of an ordinary earnings

Notification Requirements Arising Under Other Regulatory Regimes

U.S. public companies will need to assess their disclosure obligations under other regulatory regimes, which may lead them to make required disclosures about cybersecurity incidents. For example, all U.S. states, certain federal statutes, the EU and many foreign countries may require consumers or others to be notified when their personal or sensitive information has been compromised in a cybersecurity incident.

Below we discuss a number of notification regimes, including U.S. state notification laws, U.S. sector-specific regulations, MAR and GDPR, which may require a company to issue notifications or make a public disclosure in the event of a cybersecurity incident.

U.S. State and Federal Notification Laws

By and large, outside of sector-specific regulations, data protection in the United States is left to the individual states. As of June 1, 2018, with Alabama enacting its data privacy statute, all 50 states, the District of Columbia, and the territories of Guam, Puerto Rico and the U.S. Virgin Islands have enacted privacy regimes. Despite some differences, the statutes generally follow a similar structure for notification requirements, defining types of data to be protected and the circumstances when notice is required. These state laws make notification requirements applicable to any entity that retains or processes information for residents of the respective states.[10]

All states require disclosure when a cybersecurity incident compromises traditional personal identifying information such as credit card information and social security numbers, and other statutes are even more expansive. Some states require notice in as short as 15 days, and others provide no specific timeframe.[11] Still other states require that notice is provided to certain law enforcement agencies even before notice is provided to residents, or in as little as 48 hours in some circumstances.[12] Certain state laws provide exceptions to the notification obligations if the lost data was sufficiently encrypted and unreadable, or if the risk of harm from a cybersecurity incident is minimal.[13]

Some U.S. companies may also be subject to sector-specific cybersecurity and privacy laws and regulations that require disclosures of a cybersecurity incident, including:

- the Gramm-Leach-Bliley Act Financial Privacy Rule ("GLBA"),[14] which applies to financial institutions that collect nonpublic personal information from consumers;
- the HIPAA Privacy Rule, which applies to companies that electronically transmit protected health information;
- the New York Department of Financial Services ("DFS") Cybersecurity Regulation, which applies to banks, insurance companies and other financial services institutions regulated by DFS; and

forecast does not trigger any duty to update."); *In re Burlington Coat Factory Securities Litigation*, 114 F.3d 1410, 1433 (3d Cir. 1997); *In re Duane Reade Inc. Securities Litigation* No. 02 Civ. 6478 (NRB), 2003 WL 22801416, at *7 (S.D.N.Y. Nov. 25, 2003), aff'd sub nom. *Nardoff v. Duane Reade, Inc.*, 107 F. App'x 250 (2d Cir. 2004) ("company has no duty to update forward-looking statements merely because changing circumstances have proven them wrong").

[10] E.g., Massachusetts Gen Laws ch. 93H, § 3b (applicable to any entity that "owns or licenses data that includes personal information about a resident of the commonwealth").

[11] *Compare* Cal. Health & Safety Code § 1280.15 (15 days for certain medical information) with Ga. Code § 10-1-910 et seq. (providing no specific timetable).

[12] Minn. Stat. § 325E.61(2).

[13] *See, e.g.*, Fla. Stat. § 501.171.

[14] Under the GLBA, notice needs to be given to consumers in a "clear and conspicuous manner" after a possible incident involving unauthorized use or access of customer information. The GLBA also requires the impacted financial institution to notify its federal regulator in certain circumstances involving sensitive customer information.

- the Payment Card Industry Data Security Standard, which applies to any U.S. company that processes credit cards.

MAR's Disclosure Requirements

The disclosure requirements under MAR generally apply to U.S. companies with debt, equity or other securities admitted to trading on EU-regulated markets or multilateral trading facilities (or for which a request for admission to trading has been made) and companies with such securities traded on an EU-organized trading facility. If subject to MAR, a company is under an obligation to disclose to the public as soon as possible any inside information, *i.e.* nonpublic information "of a precise nature," relating directly or indirectly to the company or its financial instruments, which, if disclosed, would be likely to have a significant effect on the price of the company's securities. This differs from U.S. securities law obligations, which, as discussed above, generally do not include a continuous obligation to disclose material information to the market. Although assessing when inside information arises for purposes of MAR is fact-driven and issuer-specific, information about a cybersecurity incident may significantly impact the share price, in particular for companies in certain types of industries, and thus trigger a disclosure obligation.

Companies will need to assess carefully whether and when inside information arises, mostly focusing on the "precise nature" and "price sensitivity" of a cybersecurity incident.[15] Considering the increasing importance of data across industries, serious cybersecurity incidents involving personal data will often qualify as "inside information" for purposes of MAR. The fact that a company that has suffered a cybersecurity incident has not yet been able to assess the full extent and scale of the incident does not necessarily mean that there is no inside information.[16]

However, if and when disclosure is made, it must be done in a manner "which enables fast access and complete, correct and timely assessment of the information by the public." In the context of a cybersecurity incident, the requirement to disseminate information that allows for such a complete and correct assessment by the public will need to be carefully balanced against remaining uncertainties about the scope and nature of the incident at the time of the disclosure and possible adverse effects of too detailed a disclosure on the impacted individuals or the progress of the investigation. Consequently, it may be necessary to clearly indicate in the initial disclosure that further details will follow. In any event, issuers are required to update previous disclosures if they become aware of new inside information that renders the previous disclosure inaccurate or misleading to the public.

Under MAR, a company may decide to defer the disclosure of inside information if (i) the immediate disclosure is likely to prejudice its legitimate interests, (ii) the deferral is not likely to mislead the public and (iii) the confidentiality of the inside information can be ensured.[17] In many cases, immediate public disclosure of a cybersecurity incident will be likely to prejudice the company's legitimate interests, not only by hampering its ability to map the scale of a cybersecurity incident, identify the nature, sensitivity and volume of the affected personal data and the number of affected individuals, but also by prejudicing its ability to take effective measures to contain the incident and prevent further incidents and

[15] For companies with only straight debt (*i.e.* not convertible debt) admitted to trading in the EU, the disclosure threshold may be higher. The inside information assessment and related disclosure obligations should generally only apply to, and be understood in the context of, those debt instruments admitted to trading in the EU. Any determination of whether a cybersecurity incident amounts to inside information would appropriately focus on the relevance of the information to a debt investor. For a more detailed discussion, see our prior alert memorandum: https://www.clearygottlieb.com/news-and-insights/publication-listing/market-abuse-regulation-impact-on-us-public-companies.

[16] In light of the Geltl judgment, a "realistic prospect" that a set of circumstances may come into existence, or that an event may occur, is enough (ECJ, June 28, 2012 (Geltl v. Daimler AG), C-19/11).

[17] *See* ESMA Guidelines of October 20, 2016.

dissemination of the affected personal data. Whether the deferral is likely to mislead the public will depend on the relevant facts and circumstances. If there have been rumors in the press about a possible cybersecurity incident or statements by management regarding the robustness of the company's security systems, these circumstances may be relevant factors to consider in determining whether deferral would be likely to mislead the public. In such case, the confidentiality may also be compromised. Whether confidentiality can be ensured will also partly depend on any of the other disclosure obligations to which a company may be subject.

If disclosure is deferred, any further selective disclosure of the inside information is prohibited, except within the "normal course of professional duties" and subject to a contractual or legal confidentiality obligation. The company must be able to ensure the confidentiality of the relevant inside information at all times. Once confidentiality of the inside information can no longer be ensured, MAR requires immediate public disclosure.

GDPR's Disclosure Requirements

GDPR went into effect on May 25, 2018. GDPR applies to the processing of personal data either (i) in the context of the activities of a company's establishment in the EU (or in a place where EU law applies by virtue of public international law), regardless of whether the processing takes place in the EU or (ii) for any company not established in the EU, if the personal data processed relates to data subjects in the EU and where the processing activities relate to the offering of goods or services to those data subjects or to the monitoring of their behavior (where the behavior takes place within the EU).

The primary trigger for disclosure requirements with respect to a cybersecurity incident under GDPR is the occurrence of a "personal data breach," which is defined broadly in GDPR as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[18] GDPR requires a company to notify the competent national data protection authority ("DPA") of a cybersecurity incident without undue delay (if feasible, within 72 hours), unless the incident "is unlikely to result in a risk to the rights and freedoms of natural persons."[19]

If a decision is taken to defer MAR disclosure (see above), a notification to a DPA will be considered to fall within the "normal course of professional duties" exemption for selective disclosure of inside information of MAR and relevant personnel of the DPA will be subject to a statutory confidentiality obligation.[20]

When a cybersecurity incident is likely to result in a high risk to the rights and freedoms of natural persons, GDPR also requires a company to notify the affected individuals without undue delay. The threshold for notification to individuals is therefore higher than that for a notification to the DPA. The DPA will in many cases be able to assist in assessing whether notification to the individuals is necessary.

The individual notifications must be done in "clear and plain language" and must ensure that those notified understand the scope and significance of the

[18] Under GDPR, "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1) GDPR). Cybersecurity incidents may involve the disclosure of mixed data sets containing information that qualifies as personal data and other information that does not and therefore is not directly covered by GDPR's provisions and principles.

[19] Some EU Member States (Germany, Italy, the Netherlands) already have similar national cybersecurity incident notification requirements in place independently from GDPR.

[20] *See* Article 54(2) GDPR.

cybersecurity incident and are informed about ways to protect their personal data from further unauthorized use. If a high risk to the rights and freedoms of natural persons is identified, a company may forego directly notifying the affected individuals only if: (i) it implements or had already implemented appropriate technical and organizational protection measures (such as data encryption using state of the art algorithms) to ensure that affected personal data is protected and the risk for individuals is unlikely to materialize in practice, (ii) it has taken steps immediately following the cybersecurity incident to effectively extinguish the high risk, or (iii) notifying the affected individuals would involve a "disproportionate effort" by the company. Where notifying the affected individuals would involve a "disproportionate effort," the company must however still issue a public statement (or take other equivalent measures) to ensure affected individuals are made aware of the cybersecurity incident. In exceptional circumstances, it may even be necessary to notify the affected individuals before the competent DPA can be notified, for instance where an imminent threat of identity theft has been identified.

Notifications to affected individuals cannot be made subject to a confidentiality requirement and, in any event, confidentiality of the information cannot be ensured once a significant number of affected individuals has been notified of the fact that their personal data has been breached. At that point, the company can therefore no longer defer public disclosure under MAR and will need to make the inside information public simultaneously with the GDPR notification of the cybersecurity incident. The content of the disclosure and the level of detail to be provided to the public under MAR will however differ on a number of points from what GDPR requires to be provided to directly affected individuals.[21]

Contractual Arrangements and Voluntary Disclosures

U.S. public companies will also need to consider obligations under contractual arrangements with vendors, suppliers and other third parties, as well as reputational risk more broadly, when evaluating whether to disclose a cybersecurity incident. Parties to commercial arrangements negotiate provisions requiring a counterparty to provide notice in the event such counterparty's system has been breached in a way that may affect the other's data. Additionally, some companies, because of the nature of their business or the type of data that has been compromised, may make voluntary disclosures to inform their customers or business partners about a breach. Therefore, companies may make disclosures about cybersecurity incidents even in the absence of a specific statutory or regulatory requirement to do so.

Regulation FD and the Prohibition on Selective Disclosure

When disclosure of a cybersecurity incident is made under the various regulatory regimes described above or for other reasons, a U.S. public company will need to be mindful of the application of the SEC's Regulation FD, which prohibits public companies from selectively disclosing material nonpublic information to certain categories of individuals, including market professionals and investors under circumstances where it is reasonably foreseeable that the investors will trade on the basis of the information.[22] While "materiality" is not defined in Regulation FD, the SEC and relevant case law have

[21] For GDPR's requirements in this respect, see also the Article 29 Working Party Guidelines on personal data breach notification under Regulation 2016/679, adopted on October 3, 2017, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=47741.

[22] A number of jurisdictions have implemented similar regulations. For example, Article 3(a) of Directive 2003/6/EC of the European Parliament and of the Council on insider dealing and market manipulation (market abuse). The directive goes on to require that "whenever an issuer, or a person acting on behalf or for his account, discloses any inside information to any third party in the normal exercise of his employment, profession or duties,... he must make complete and effective public disclosure of that information, simultaneously in the case of an intentional disclosure and promptly in the case of a non-intentional disclosure" (as discussed below). Article 3(a) of Directive 2003/6/EC of the European Parliament and of the Council on insider dealing and market manipulation (market abuse) at Article 6(3).

provided guidance about its meaning.[23] Importantly, the Commission clarified in its 2018 interpretive guidance that Regulation FD's prohibition on selective disclosure may include information relating to a material cybersecurity incidents.

Regulation FD does not prohibit disclosures made to persons who are bound by duties of trust or confidence to not disclose or to not use the material nonpublic information for trading, including persons who have explicitly contracted to maintain the information as confidential. Therefore, U.S. public companies need to determine whether disclosure under any regulatory regime, contractual arrangement or voluntary disclosure is subject to confidentiality and, if not, need to make the broader public disclosure required by Regulation FD.

Takeaways

Upon the occurrence of a cybersecurity incident, a U.S. public company needs to consider whether it has disclosure obligations under the U.S. federal securities laws, U.S. state notification laws, U.S. sector-specific regulations, MAR, GDPR and other applicable laws or regulations. Likewise, a company may be under a contractual obligation to disclose, or may choose to make a voluntary disclosure regarding, the cybersecurity incident. In the event the cybersecurity incident is disclosed only selectively to certain parties, the company will also need to be mindful of whether public disclosure would then be required by Regulation FD. Each of these potential obligations must be carefully considered and analyzed, particularly as regulators around the world continue to focus on the adequacy of company responses to material cybersecurity incidents, including compliance with disclosure obligations.

…

CLEARY GOTTLIEB

[23] *See* "Understanding U.S. Disclosure Requirements" above for a discussion on generally applicable standards of materiality.