Human life is increasingly digitized. Intimate details of peoples’ lives are stored on social media platforms and a multitude of electronic databases. The so-called “Internet of Things” means that even thermostats and blood-glucose meters now collect and transmit personal data. Ride-sharing apps like Uber and Lyft track riders’ destinations and departure times.

While the new digital world holds much promise, personally identifiable information (PII) and other sensitive, private data are increasingly at risk, as hackers target security weaknesses for illicit profit or other nefarious purposes. And data breaches are expensive; a recent study by the Ponemon Institute found that the average cost of each lost or stolen record is $141. Globally, the average total cost of a breach was found to be $3.62 million.

As the potential harm from data breaches increases, and the public becomes more aware of that risk, data breaches may have significant effects on the share price of publicly traded corporations. This, in turn, means that government regulators will increasingly scrutinize whether corporations have adequately disclosed information related to data security, or whether insiders have inappropriately traded on nonpublic information related to data breaches. Meanwhile, the lack of clear guidance on the topic and the complex factual scenarios in which data breaches occur create challenges for counsel advising businesses and executives about how to best respond to data breaches.

Recent high-profile data breaches provide valuable lessons regarding how lawyers and executives should approach data breaches, even as new questions are raised. From a securities law perspective, one challenge is that whether a breach must be disclosed depends on whether it is considered material, which in turn depends in part on how the breach is viewed by the market. As awareness of the risks of data breaches increases, investors may increasingly view data breaches as material to share price, which likely will result in more scrutiny from the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) of potential disclosure and insider trading cases connected to data breaches.

THE EQUIFAX AND UBER DATA BREACHES, AND THE INTEL DESIGN FLAW

The Equifax data breach is among the most far reaching data breaches so far. According to its website, Equifax “assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide.” On September 7, 2017, Equifax revealed that sensitive personal information of 143 million Americans was exposed in a data breach. According to Equifax, the illegally accessed
data includes names, Social Security numbers, birth dates, addresses, and driver’s license numbers. For a smaller number of consumers, hackers also accessed credit card numbers and “certain dispute documents” containing PII.

Although not nearly as far-reaching as the Equifax data breach, in November 2017 Uber announced a data breach that may be the most widely publicized breach involving a private company. According to Uber’s statement on the breach, the company became aware in 2016 that “two individuals outside the company had inappropriately accessed user data stored on a third-party cloud-based service.” The breach included the names and driver’s license numbers for 600,000 Uber drivers, as well as names, e-mail addresses, and phone numbers for 57 million Uber users.

More recently, in January 2018, Intel revealed a major security flaw in the design of its chips, which potentially exposed a huge number of computers and mobile devices to data breaches. Its share price dropped sharply after the disclosure. Moreover, it was reported that Intel had known about the issue since June 2017, but had delayed disclosure for six months. In addition, Intel’s CEO Brian Krzanich had sold nearly all his shares in the company in late November 2017, about a month before the disclosure.

RELEVANT SECURITIES LAWS: A VERY BRIEF OVERVIEW

The Securities Act of 1933 and the Securities Exchange Act of 1934 provide broad protections to investors. In certain cases, they may require companies to disclose information about data breaches or other information security issues. A typical securities action will involve a claim under section 10(b) of the Exchange Act, which broadly prohibits fraud in connection with the sale of securities. Although the securities laws do not create a general duty to disclose, a company may need to disclose information about a data breach if necessary to prevent a statement from being misleading. For example, if a breach is expected to lead to significant legal costs or reputational harm, a company might need to disclose the breach to prevent forward-looking statements about financial performance from being misleading.

A publicly traded company may also need to disclose a data breach in the management discussion and analysis (MD&A) section of the company’s periodic reports. According to SEC guidance, the MD&A should address data breaches or other information security risks if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant’s results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.

The antifraud protections of section 10(b), as interpreted by SEC Rule 10b5-1, also prohibit insider trading, i.e., “the purchase or sale of a security . . . on the basis of material nonpublic information.” Likewise, section 20A of the 1934 Act creates a private right of action that allows investors to sue insiders who have traded on material, nonpublic information. Insider trading laws may be implicated where insiders know about a breach and believe that it will have an effect on share price once the information becomes public. Trading on such nonpublic information could result in civil and criminal liability.

Under any of these laws, a critical question will be whether a data breach is material. As discussed below, evaluating the materiality of a data breach can be tricky, especially given the evolving factual and legal issues related to data breaches, and the flexible standard for materiality the US Supreme Court has adopted.

LESSONS ON MATERIALITY FROM THE EQUIFAX DATA BREACH

The Equifax data breach provides some helpful lessons regarding materiality and the considerations involved in determining whether and when to disclose a breach. Equifax has stated that it first discovered a massive data breach on July 29, 2017. As it has been widely reported, executives sold a total of almost $1.8 million worth of Equifax shares a few days after the breach. Weeks later, when the data breach was publicly announced, the price of Equifax shares dropped precipitously. Equifax has stated that the executives who sold the shares did not know about the data breach at the time of the sale. Nonetheless, it has been reported that the DOJ and SEC are investigating the stock sales as potential insider trading.

Evaluating potential liability for insider trading in the context of a data breach is complicated by the malleability of the legal standard for materiality and the difficulty of assessing the seriousness of a data breach. A critical question in insider trading cases is whether the information possessed by the insider is material. The US Supreme Court has rejected a bright-line rule for whether information is material. (Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27 (2011); Basic Inc. v. Levinson, 485 U.S. 224 (1988)). Rather, information is material when the reasonable investor would view the information as significantly altering the “total mix” of the information available. Assessing materiality, therefore, is always a “fact-specific inquiry.” (Matrixx, 563 U.S. at 43.)

Not every “adverse event” must be disclosed. Similarly, an insider’s knowledge of a nonpublic adverse event will not necessarily give rise to a claim of insider trading. For example, in the context of reported side effects of pharmaceuticals, the US Supreme Court explained that “[a]dverse event reports are daily events in the pharmaceutical industry.” (Id.) Likewise, information security intrusions are relatively common events. For example, the Identity Theft Resource Center reported that it tracked 1,093 data breaches in the United States in 2016. Given that data breaches are relatively common and vary in severity, it is likely that a relatively small percentage of data breaches will rise to the level of material under the “total mix” standard.

The uncertainty created by the flexible “total mix” standard is compounded by the factual uncertainty that companies face...
when initially evaluating the severity of a data security issue. A review of the timeline of the Equifax data breach—as described by former CEO Richard Smith in his congressional testimony—raises the question of exactly when insiders at Equifax had information about the breach that might support the conclusion that it would be “material.”

- According to Smith, Equifax, along with other companies, received information about a vulnerability in software called Apache Struts on March 8, 2017.
- On March 9, Equifax notified its personnel about this vulnerability, but for some reason Equifax failed to appropriately patch the vulnerability.
- On July 29, Equifax observed “suspicious network traffic associated” with its consumer dispute website. Equifax “investigated and immediately blocked the suspicious traffic that was identified.”
- On July 30, Equifax “observed additional suspicious activity” and “took the web application completely offline.”
- On July 31, Equifax’s chief information officer informed Smith about the “suspicious activity.” Specifically, Smith testified that he “was informed that there was evidence of suspicious activity on our dispute portal and that the portal had been taken offline to address the potential issues.” While the issue was apparently known to be serious enough to warrant the attention of the CEO, Smith testified that, at that time, he “certainly did not know that [PII] had been stolen, or have any indication of the scope of this attack.”
- On August 2, Equifax retained a law firm and a forensic consulting firm, and contacted the FBI.
- By August 11, the ensuing investigation revealed that the hackers may have accessed a large amount of consumer PII.
- On August 15, Smith was informed that “it appeared likely that consumer PII had been stolen.”
- By September 4, “the investigative team had created a list of approximately 143 million consumers whose personal information” had been stolen.
- Finally, on September 7, Equifax publicly announced the data breach.

It is far from clear at exactly what point the information known to insiders at Equifax about the data breach might arguably have become material under the “total mix” standard. The possible insider trading being investigated occurred early in the timeline, before the severity of the breach may have been understood. On the other hand, as one of the “Big Three” consumer credit reporting agencies, Equifax is in the business of collecting and aggregating sensitive consumer information. Any substantial data security intrusion raises the possibility of significant reputational harm or regulatory action. Undoubtedly, part of the government’s investigation will look at what reasonably could have been inferred from the facts Equifax initially knew about the security intrusion.

**UBER, YAHOO, INTEL, AND THE CONSEQUENCES OF DELAYED DISCLOSURE**

While Equifax has been criticized for the time it took to disclose the security breach, Yahoo and Uber provide more extreme examples. Uber admitted that it covered up a 2016 data breach by paying hackers to keep quiet and to supposedly delete the stolen data. The breach, which occurred in October 2016, was revealed more than a year later, after Uber’s former CEO stepped down and was replaced by a new CEO, Dara Khosrowshahi, who was reportedly told about the breach two months before Uber disclosed it publicly.

Uber’s failure to disclose the breach is being challenged under state laws. In addition, Uber was already under investigation by the Federal Trade Commission (FTC) for separate breaches in 2014. Uber settled the action the FTC brought against it regarding the 2014 breaches in August 2017. If Uber made misstatements about the 2016 breach during the course of the investigation of the 2014 breach, it could face potential criminal charges.

As a result of the breach and its aftermath, Uber fired its chief security officer, a former federal prosecutor. Uber also fired its legal director of security and law enforcement. Not surprisingly, Uber has already been sued by private litigants, as well as by state and local governments. The FTC and other states are investigating, and Uber has also faced sharp questions from Congress.

One interesting wrinkle in the saga of the 2016 Uber data breach is that Uber reportedly disclosed the breach to SoftBank, which was considering a multibillion-dollar investment in Uber at the time. The data breach may have been one factor that ultimately allowed SoftBank to acquire a significant piece of the company at a discount. While Uber may have hedged off the potential for a fraud or breach of contract claim by disclosing the breach to a potential investor, its decision to disclose the breach to SoftBank while withholding information about the breach from the public has raised eyebrows.

Yahoo waited even longer to disclose its massive data breach. For about two years, as reported in Yahoo’s 2016 Form 10-K, Yahoo failed to disclose that account information for 500 million accounts had been stolen in 2014. Yahoo did not disclose the 2014 breach until September 2016. According to the Form 10-K, its “information security team had contemporaneous knowledge of the 2014 compromise of user accounts, as well as incidents by the same attacker involving cookie forging in 2015 and 2016.” While the company took certain remedial efforts, “it appears certain senior executives did not properly comprehend or investigate, and therefore failed to act sufficiently upon, the full extent of knowledge known internally by the Company’s information security team.” An independent committee of the board of directors found that “the relevant legal team had sufficient information to warrant substantial further inquiry in 2014, and they did not sufficiently pursue it.”

A grand jury recently indicted four defendants, including officers of the Russian Federal Security Service (FSB), for hacking and economic espionage for their role in the conspiracy to steal the Yahoo data. Yahoo, meanwhile, is reportedly facing an investigation by the SEC regarding its delayed disclosure of the breach. The company also announced in its Form 10-K that it was “cooperating with federal, state, and foreign governmental officials and agencies” regarding the 2014 breach and other data breaches.
Intel’s delay in disclosing its own issues has also drawn scrutiny. On about June 1, 2017, Google security researchers reportedly advised Intel regarding vulnerabilities in its chips, which can enable hackers to breach devices containing them. On October 30, 2017, CEO Krzanich implemented a stock sale plan that involved executing options and share sales that decreased his holdings in the company by about 50 percent, down to the minimum allowed under the company’s ownership requirements. On November 29, the plan was executed, resulting in over $39 million in proceeds. The company did not release a statement on the security issue until January 3, 2018; its shares declined over 5 percent. Several members of Congress have called on the SEC and DOJ to open investigations into the incident, while several shareholder class actions have already been filed.

The Yahoo, Uber, and Intel cases involved significant delays in disclosing massive data breaches. While those companies may arguably have waited too long to disclose their respective data breaches, more typical cases may involve difficult questions about what to disclose and when.

A LACK OF GUIDANCE, BUT INCREASING AWARENESS

The difficulty in assessing the materiality of a data breach or other information security incident is complicated by both legal and factual uncertainty. In 2011, the SEC published guidance on “disclosure obligations relating to cybersecurity risks and cyber incidents.” While the guidance offers some help, it raises as many questions as it answers. The guidance states that material cybersecurity risks and incidents should be disclosed, and it provides general examples of what might constitute a material data breach. Nonetheless, many questions are left unanswered with respect to assessing the materiality of a particular incident, which will turn on the specific factual context in which the breach occurred. (Executives facing the challenges of a data breach may take heart that even the SEC has been a victim. The SEC reported in a statement by Chairman Jay Clayton that it learned in August 2017 that a cybersecurity “incident previously detected in 2016 may have provided the basis for illicit gain through trading.” As in the Equifax case, a “software vulnerability” that was later patched had allowed “access to nonpublic information.”)

It is also difficult to assess materiality because the evolving legal landscape creates uncertainty about whether and to what degree companies will be exposed to liability for a breach. This lack of certainty is evident in the circuit split regarding whether consumers have standing to bring a lawsuit in federal court following a data breach. For example, a recent Eighth Circuit decision held that allegations of future injury were not sufficient to confer standing. (In re SuperValu, Inc., 870 F.3d 763, 772 (8th Cir. 2017).) Other circuits have come to the opposite conclusion, although the decisions may have “turned on the substance of the allegations before each court.” (Id. at 769.) Recent high-profile data breaches may also result in legislation that would significantly increase the penalties for failing to disclose a data breach. For example, Senator Bill Nelson has introduced the Data Security and Breach Notification Act, which would require companies to notify consumers of a data breach within 30 days of the discovery of the breach, unless the company could show that notification within that timeframe would be infeasible or would compromise data security. The proposed legislation would also create new criminal penalties for deliberately concealing a breach. More recently, Senators Elizabeth Warren and Mark Warner introduced the Data Breach Prevention and Compensation Act, which is aimed at credit reporting agencies like Equifax.

In addition to the legal issues involved with assessing a data breach, factual uncertainty abounds. As discussed above, many factual questions must be answered in the immediate aftermath of a data breach. More broadly, it may be difficult to assess the costs of a data breach. As discussed in an International Monetary Fund working paper entitled “Cyber Risk, Market Failures, and Financial Stability,” direct costs, such as forensic investigation and post-breach security measures, may be relatively easy to assess. Indirect costs, such as reputational harm or the devaluation of intellectual property, are likely to be much more difficult to determine. While insurance can offset some costs, it is unlikely to cover longer-term, indirect harm. Harm, of course, will also depend on the type of data stolen. For example, Uber has reported that there is no indication “that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded.” But even seemingly innocuous data can be used as bait in phishing schemes. Moreover, the reputational harm to Uber, which has already been in the crosshairs for unrelated matters, may be incalculable.

CONCLUSION

As a consumer reporting agency, Equifax may have been particularly vulnerable to the effects of a data breach. As a digital ride-sharing business that has, of late, been in the news for the wrong reasons, Uber, too, may have been particularly at risk. Similarly, Intel is a dominant player in the IT hardware industry, and thus any security issues with its products have a broad impact. The information economy, however, means that many companies now collect and store sensitive data as a critical part of their business. Recent high-profile data breaches—and the attention they have received from investors, legislators, and the public—may suggest that data breaches will increasingly become material events, triggering duties to disclose or to refrain from trading. Increasing publicity surrounding data breaches may also raise the interest of the DOJ and SEC in investigating disclosure and insider trading cases connected to data breaches. However, even when the law regarding liability for data breaches matures, government investigations will be complicated by the interplay between materiality and knowledge.