Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

10 Questions The SEC Will Probably Ask Google: Part 2

By **John Reed Stark** (October 10, 2018, 3:04 PM EDT)


John Reed Stark

Having served for over 11 years as chief of the U.S. Securities and Exchange Commission's Office of Internet Enforcement and almost 20 years in the SEC enforcement division in total, I have a unique perspective into the cyber-related priorities of the SEC enforcement division. But one does not need to have my experience to predict that the SEC is probably investigating Google's recent announcement that it will close most of its failing social media platform, Google+, and implement several new privacy measures because of a previously undisclosed software bug relating to its Google+ application programming interface.

One need only review a speech given about a year ago by Stephanie Avakian, the co-director of the SEC Enforcement Division, titled, "The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity."

In her speech, the seasoned Avakian offers a lengthy and detailed road map of the SEC's cyber priorities, including cyber-related disclosure failures by public companies. In her speech, Avakian states:

> In an era where nearly every company is dependent on computer systems to operate their business, it is frequently necessary to provide meaningful and timely disclosures regarding cyber risks and incidents. These disclosures are often material on their own or necessary in order to make other disclosures, in light of the circumstances under which they are made, not misleading. We recognize this is a complex area subject to significant judgment, and we are not looking to second-guess reasonable, good faith disclosure decisions, though we can certainly envision a case where enforcement action would be appropriate.

About six months later, the SEC brought its first enforcement action involving a cyber disclosure failure against the entity formerly known as Yahoo, which agreed to pay a $35 million penalty to settle charges that it misled investors by failing to disclose its data breach in which hackers stole personal data relating to hundreds of millions of users. Steven Peikin, Avakian's co-director of SEC enforcement, stated in the SEC's announcement of the settlement:

> We do not second-guess good faith exercises of judgment about cyber-incident disclosure. But we have also cautioned that a company's response to such an event could be so lacking that an enforcement action would be warranted. This is clearly such a case.

Jina Choi, director of the SEC's San Francisco regional office and who led the SEC's investigation of Yahoo, added:

> Yahoo's failure to have controls and procedures in place to assess its cyber-disclosure obligations ended up leaving its investors totally in the dark about a massive data breach. Public companies should have controls and procedures in place to properly evaluate cyber incidents and disclose material information to investors.

Google's announcement notes that up to 500,000 Google+ users potentially had their personal

Google's announcement notes that up to 500,000 Google+ users potentially had their personal data exposed. In addition, Google reported that up to 438 applications may have used the defective Google+ API, which makes estimations of impacted individuals difficult to ascertain. Meanwhile the Wall Street Journal and the Washington Post reported that Google hid the Google+ API defect from shareholders and others for fear of regulatory examination, congressional inquiry and other negative ramifications.

Clearly, Google's situation could be what Avakian, Peikin and Choi had in mind with respect to their concerns and priorities — it all depends on what the SEC discovers during its investigation.

But what precisely will the SEC ask of Google? Assuming I am right about an ongoing SEC investigation, this two-part series presents 10 questions SEC enforcement staff will be posing to Google executives and others in connection with an investigation of Google's public disclosures of the Google+ API defect.

Part one discussed: (1) some critical background on the SEC's disclosure requirements when it comes to cybersecurity risks and events; and (2) the first five of 10 general questions that Google will likely have to answer if the SEC investigates.

Part two picks up right where part one left off, beginning with question number six and finishing the 10-question list that Google will likely have to answer if the SEC investigates. Here, I also share some final thoughts, looking ahead for Google and its current predicament.

6. How long did it take for Google to remediate after discovery of the data security vulnerability?

Good news on this front for Google. Google should take some comfort that the SEC's 2018 guidance on cybersecurity disclosure recognizes that data security incident investigations are complicated and cannot be completed overnight.

The SEC recognizes that the investigation of data security incidents can take time, and that some companies may not want to make any disclosures about an incident when they do not have some comfortable handle on the facts of the situation. The 2018 SEC guidance states:

> Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident. We also recognize that it may be necessary to cooperate with law enforcement and that ongoing investigation of a cybersecurity incident may affect the scope of disclosure regarding the incident.

But the SEC also qualifies its recognition of the complexity of data security incidents and warns companies that the need for a lengthy investigation into a data security incident is not necessarily an automatic excuse for delaying the disclosure of a data security incident, stating, "However, an ongoing internal or external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident."

Of course, when a data security incident happens, the public's demand for immediate answers is understandable. Life savings are at risk while the perpetrators of hacking schemes are rarely identified, let alone captured and prosecuted. However, in the aftermath of most data security incidents, there exists no CSI-like evidence that would allow for speedy evidentiary findings and rapid remediation.

While some data security incidents may provide key evidence early on, most never do, or even worse, provide a series of false positives and other stumbling blocks. The evidence among the artifacts, remnants and fragments of a data security incident is rarely in plain view; it can rest among disparate logs (if they even exist), volatile memory captures, server images, system registry entries, spoofed IP addresses, snarled network traffic, haphazard and uncorrelated time stamps, internet addresses, computer tags, malicious file names, system registry data, user account names, network protocols and a range of other suspicious activity.

Moreover, evidence can become difficult to nail down — logs are destroyed or overwritten in the course of business, archives become corrupted, hardware is repurposed, and the list goes on.

For instance, in Google's case, according to the Wall Street Journal, certain key logs were simply never retained, which created obstacles for its internal investigators:

> Because the company kept a limited set of activity logs, it was unable to determine which users were affected and what types of data may potentially have been improperly collected, the two people briefed on the matter said. The bug existed since 2015, and it is unclear whether a larger number of users may have been affected over that time.

In short, the evidence analyzed during a data security incident can be a massive, jumbled and a chaotic morass of terabytes of data. That is why the investigation of a data security incidents can take weeks, perhaps months, before any concrete conclusions begin to take shape. Rushing to judgment (and disclosure) might not only create further confusion and expense, but it can also undermine the objectivity, truth and confidence that the public (especially shareholders) deserves.

7. Did Google undertake a timely and comprehensive disclosure of its data security incident?

The Wall Street Journal reported one blockbuster fact that will be a lightning rod for SEC enforcement attention: "[Google] opted not to disclose the issue this past spring, in part because of fears that doing so would draw regulatory scrutiny and cause reputational damage."

The SEC will likely begin its investigation by reviewing Google's disclosures since March 2018, when a privacy task force formed inside Google, code-named Project Strobe, apparently discovered the API problem during a companywide audit of the company's APIs. Google's announcement states, "We discovered and immediately patched this bug in March 2018. We believe it occurred after launch as a result of the API's interaction with a subsequent Google+ code change."

The 2018 SEC guidance clearly emphasizes the need for timely disclosure, probably taking a lesson from the Equifax data breach and, ironically, from the SEC's own data breach experience, which SEC Chairman Jay Clayton admitted should have been disclosed earlier.

Equifax, one of the three elite repositories of personal credit information and a trusted source for personal security and identity theft defense products, disclosed a cyberattack that could potentially affect 148 million consumers — nearly half of the U.S. population. The accessed Equifax data reportedly included sensitive information such as Social Security numbers, birthdays, addresses and, in some instances, driver's license numbers — a virtual treasure trove for identity thieves.

Not long after the Equifax data breach, Clayton also announced a data breach into the SEC's EDGAR system, a vast database that contains information about company earnings, share dealings by top executives, and corporate activity such as mergers and acquisitions. Accessing that information before it's disclosed publicly could allow hackers to profit by trading ahead of the information's release.

With respect to the Equifax data breach, now "retired" Equifax CEO Richard Smith told a breakfast meeting in August 2017 that data fraud is a "huge opportunity," allowing Equifax to sell consumers more offerings. Smith touted the company's credit-monitoring offerings, according to a video recording of the meeting at the University of Georgia's Terry College of Business, and declared that protecting consumer data was "a huge priority" for the company.

But what the Equifax CEO failed to mention was that less than three weeks earlier, Equifax had apparently discovered a potentially massive data security incident and that Equifax had called in expert incident response firm Mandiant to investigate. Yet, it was not until a few weeks later, on Sept. 7, 2017, that Equifax disclosed the massive data breach to the public.

With respect to the SEC data breach, the agency itself may have opted for a similar path of delayed notification. Reports and Clayton's testimony before the Senate Banking Committee indicate that the SEC data breach was discovered in 2016, and the possible illegal trades were detected in August 2017, but the SEC did not disclose any information about the incident until Sept. 20, 2017.

Sept. 20, 2017.

Senior executives at both the SEC and Equifax have angered their constituents with their arguably sluggish disclosure. Both entities probably focused too much upon what they were legally and contractually obligated to disclose, rather than taking a more holistic approach to the question.

Per the 2018 SEC guidance, if Google learned of a cybersecurity incident or cyber risk that was material to its investors, then Google was expected to make appropriate disclosures. The guidance even goes so far as to remind public companies to consider obligations under the stock listing requirements, such as Section 202.05 of the New York Stock Exchange Listed Company Manual and Nasdaq Listing Rule 5250(b)(1). Additionally, the 2018 SEC guidance emphasizes the possible need to "refresh" previous disclosures during the process of investigating a cybersecurity incident or past events.

When organizing the disclosure of data security incidents and overall cybersecurity risks, just like the SEC's 2011 guidance, the 2018 guidance explains that disclosure of data security incidents may be required in sections of public filings addressing risk factors, management discussion and analysis, description of business, legal proceedings and financial statement disclosures.

No doubt, SEC enforcement staff will be poring over these various sections of disclosure, looking for any possibly misleading information or material omission.

8. Was there any trading by any Google personnel who knew of the data security incident?

While empirical data may suggest otherwise, some data security incidents can impact a company's stock price — for example, the actual stock price dropped immediately following disclosure of breaches at Equifax and Target. In such situations, executives who learn of a data security incident, if it is material and nonpublic, could be violating insider trading laws if they engage in any trading of the company's stock.

Along these lines, the 2018 SEC guidance warned corporate insiders not to sell shares of a company when holding confidential knowledge about cyberattacks and breaches that could affect stock price. This is an area not covered by the 2011 SEC guidance but made sense to include in the 2018 SEC guidance.

Equifax once again probably triggered the SEC's concerns and prompted inclusion of this principle in the 2018 SEC guidance. The Equifax data breach also involved a stock sell-off by some of its executives before the disclosure of its experience of a cyberattack and spurred an SEC insider trading investigation that resulted in at least one SEC enforcement action against an Equifax manager for unlawful insider trading. Intel CEO Brian Krzanich got hit with a similar backlash, too, for selling a large block of shares after learning of the Meltdown and Spectre computer chip vulnerabilities, but before disclosing them to the public.

The SEC is obviously expecting that Google has thoughtful and well-documented consideration of data security incidents in the context of possible trading on material, nonpublic information — and carefully drafted, robust and precise policies, practices and procedures in place to demonstrate a rigorous culture of compliance.

SEC enforcement staff will likely explore whether the 2018 SEC guidance prompted Google to review, with data security incidents in mind, their trade restriction policies, permissible trading windows, insider trading training curricula, codes of ethics, trade authorization procedures, trading training manuals and the like.

9. Was Google mindful of Regulation FD when briefing outsiders about its data security incident?

Regulation FD (for "Fair Disclosure") promulgated by the SEC under the Securities Exchange Act of 1934, as amended, prohibits companies from selectively disclosing material nonpublic information to analysts, institutional investors and others without concurrently making widespread public disclosure.

Regulation FD reflects the view that all investors should have equal access to a company's material disclosures at the same time. Since its enactment in 2000, Regulation FD has fundamentally reshaped the ways in which public companies conduct their conference calls, group investor meetings and so-called "one-on-one" meetings with analysts and investors.

The SEC adopted Regulation FD to address the selective disclosure by issuers of material nonpublic information. In its adopting release, the SEC expressed concerns about reported instances of public companies disclosing important nonpublic information, such as advance warnings of earnings results, to securities analysts or selected institutional investors or both, before making full disclosure of the same information to the general public. Those privy to the information beforehand were able to profit or avoid a loss at the expense of everyone else.

The 2018 SEC guidance emphasizes that companies subject to Regulation FD (like Google) should have policies and procedures to promote compliance with Regulation FD regarding cybersecurity risks and incidents.

In particular, these policies and procedures should work to ensure that Google did not make any selective disclosures about cybersecurity risks and incidents to Regulation FD-enumerated persons without the required broadly disseminated public disclosure. This can create unanticipated problems for any public company experiencing any form of data security incident, because Regulation FD can throw a wrench into an already challenging disclosure process.

For example, in the aftermath of a data security incident of any kind, in addition to any consumer notifications, a broad range of other important notifications may immediately arise, such as briefings to customers, partners, employees, vendors, affiliates, insurance carriers, and a range of other interested or impacted parties.

Given the broad swath of interested parties, SEC enforcement staff will be looking to make sure Google maintained careful and methodical communications practices to ensure that their disclosures were consistent, and not selective.

10. Do Google's disclosures, or lack thereof, amount to criminal behavior?

Perhaps the most important takeaway from the 2018 SEC guidance is a notion not specifically stated in the four corners of the document, but rather found in an SEC enforcement action (and a parallel U.S. Department of Justice criminal prosecution) filed on the very same day of the 2018 SEC guidance's release.

In the SEC enforcement action, captioned SEC v. Jon E. Montroll and Bitfunder, the SEC charged a former bitcoin-denominated platform and its operator with operating an unregistered securities exchange and defrauding users of that exchange. The SEC also charged the operator with making false and misleading statements in connection with an unregistered offering of securities.

Among other accusations, the SEC alleges that BitFunder and its founder Jon E. Montroll operated BitFunder as an unregistered online securities exchange and defrauded exchange users by misappropriating their bitcoins and failing to disclose a cyberattack on BitFunder's system that resulted in the theft of more than 6,000 bitcoins.

The SEC actually alleges fraud because of the lack of disclosure of the data security incident to customers/account holders, effectively bypassing the issue of whether there is actually any statutory or regulatory disclosure obligation. In other words, by keeping the data security incident a secret, the exchange (which was unlawfully unregistered), committed a fraud upon its customers. The SEC complaint states:

> Montroll failed to disclose the theft [which occurred by means of a cyberattack] and the deficit to Ukyo Notes investors and potential investors. By failing to disclose these facts, Montroll misled investors and potential investors — who were led to believe they would profit, at least in part, from BitFunder's operations — to reasonably believe that BitFunder was a secure and profitable business.

Concealing a data security incident can not only prompt SEC enforcement actions but can also lead to being arrested and taken into custody. In a parallel criminal case, the U.S. Attorney's

lead to being arrested and taken into custody. In a parallel criminal case, the U.S. Attorney's Office for the Southern District of New York filed a complaint against Montroll for perjury and obstruction of justice during the SEC's investigation. In other words, whether a public company or private company and whether a regulated entity or an unregulated one, keeping a data security incident secret can be the kind of act that triggers an indictment. The SDNY's press release about their parallel case states:

> As alleged, Montroll committed a serious crime when he lied to the SEC during sworn testimony. In an attempt to cover up the results of a hack that exploited weaknesses in the programming code of his company, he allegedly went to great lengths to prove the balance of bitcoins available to BitFunder users in the WeExchange Wallet was sufficient to cover the money owed to investors. It's said that honesty is always the best policy — this is yet another case in which this virtue holds true.

Nothing in any of the few public reports of the Google+ incident indicates any clear-cut nefarious form of fraud or chicanery. However, the Wall Street Journal reports that Google failed to disclose the Google+ API defect for fear of regulatory and other ramifications, stating:

> The [internal Google] document shows Google officials felt that disclosure could have serious ramifications. Revealing the incident would likely result "in us coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal," the memo said. It "almost guarantees Sundar [Pichai, Google's CEO] will testify before Congress."

Google executives should realize that SEC enforcement staff will be looking for any hint of deception in their handling of the Google+ API defect — and that SEC enforcement staff will gladly pass along any evidence of fraud to the FBI and the DOJ.

Looking Ahead

In addition to Google's shareholders, a data security incident can trigger a litany of legal notification and disclosure requirements, including notice to state regulators, federal regulators, EU General Data Protection Regulation supervisory authorities, vendors, partners, insurance carriers, customers, consumers, employees, and any other constituency who may have a vested interest in a victim company.

Hence, it is not surprising that disclosure of cybersecurity incidents and cybersecurity risks has evolved into one of the most important program areas of SEC enforcement, mentioned in so many SEC speeches and panel discussions. Yet the SEC enforcement division has only filed one SEC enforcement action, against Altaba — formerly known as Yahoo, alleging any sort of data security incident disclosure failure. This is probably because cybersecurity disclosures are usually made in good faith and lack the kind of obvious misconduct and fraud that the SEC typically prosecutes.

But that should provide Google with little solace. The SEC enforcement division is always looking to prosecute the "big fish" to reinforce a regulatory priority or decree — and Google could fit that bill, especially if the Wall Street Journal report about Google's efforts at concealment turn out to be even slightly treacherous or outrageous.

As an aside, the Wall Street Journal report implies the existence of an active whistleblower at Google who provided inculpatory memoranda and other documents. The SEC loves whistleblowers, cultivates whistleblowers, seeks out whistleblowers, and financially rewards whistleblowers for their efforts, especially when a whistleblower is a company insider. Whoever was speaking to the Wall Street Journal regarding the Google+ API issue will probably be cooperating with the SEC soon enough.

For Google, perhaps the Google+ API defect was only a minor data mishap and an aberration, and its internal investigative team acted promptly, carefully, swiftly and in the best interest of Google shareholders to remediate the vulnerability. Only time will tell.

In the meantime, my advice is for Google to prepare itself for a vigorous and relentless SEC enforcement division investigation — and have its responses ready not just to the 10 questions cited in this two-part series, but also to the many other questions that the SEC will most certainly

pile on.

And if it has not done so by now, Google should consider engaging an independent law firm and digital forensics firm to confirm the findings of Google's privacy and data protection office and recommend future remedial actions. To me, injecting independence, transparency and sunlight into Google's process not only seems like a no-brainer, but would also contribute to a far more thoughtful, conscientious and meritorious defense.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."