Bloomberg Law Reports®

March 13, 2012

Securities Law

Federal Securities Law

Disclosure & Reporting

The Facebook IPO and Disclosure of Cybersecurity and Privacy Risks: Tips and Lessons for Practitioners


MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Contributed by Cynthia J. Larose and Adam M. Veness, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C.

The Facebook, Inc. (Facebook) initial public offering last month was probably the most anticipated IPO filing of the 21st century. In its S-1 filing with the U.S. Securities and Exchange Commission (SEC) - the first step on any company's journey to becoming a publicly traded company - Facebook has set the bar for S-1 disclosure in the areas of cybersecurity and privacy risks. [1]

Less than four months before Facebook's S-1 filing, the SEC's Division of Corporation Finance (Division) issued informal guidance regarding public companies' disclosure of cybersecurity risks and cyber incidents (Cybersecurity Guidance).[2] The Cybersecurity Guidance did not create any new disclosure requirements, but rather clarified existing law in an effort to better educate the ever-growing group of companies that face cybersecurity risks and cyber incidents in their businesses.

In its S-1 filing, Facebook fully adopts Cybersecurity Guidance, and provides a real-life example of how companies facing cybersecurity and privacy risks should disclose this information to investors. Indeed, Facebook takes the Cybersecurity Guidance a step further and even discloses risks that are associated *indirectly* with cybersecurity and privacy concerns, such as unfavorable media coverage and potential reputational damage that could result from the failure to maintain adequate cybersecurity and privacy protection. For companies trying to review and understand the Cybersecurity Guidance, much can be learned by examining Facebook's "Risk Factors" and "Business" S-1 sections.

Risk Factors[3]

In accordance with the Cybersecurity Guidance, Facebook's Risk Factors clearly explain to potential investors how cybersecurity risks and incidents could have an adverse effect on the company. The Cybersecurity Guidance explains that companies should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. In determining whether risk factor disclosure is required, the Division suggests that companies take into account all relevant information, including:

- prior cyber incidents and the severity and frequency of those incidents;
- the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks; and
- the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which the company operates and risks to that security.

If risk factor disclosure is required, the Division suggests that appropriate disclosures may include:

- discussion of those aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
- to the extent the company outsources functions that have material cybersecurity risks, descriptions of those functions and how the company addresses those risks; and
- descriptions of cyber incidents experienced by the company that are individually, or in the aggregate, material, including a description of the costs and other consequences.

The Division also cautions companies to avoid boilerplate and generic risk factors. Companies should ensure that they adequately describe the nature of the material risks and specify how each risk affects the company.

Facebook has done just that. Rather than making mere general disclosures about cybersecurity and privacy risks for internet businesses, Facebook tailors its Risk Factors specifically to Facebook. By analyzing different aspects of Facebook's Risk Factors, other companies facing cybersecurity, cyber incidents, and privacy risks can use the Facebook S-1 as a roadmap for preparing their own risk factors.

– Investigations

Facebook's Risk Factors extensively discuss details about prior investigations by the Federal Trade Commission (FTC) and the Irish Data Protection Commissioner (DPC). The disclosure explains the specifics of a 20-year settlement agreement between Facebook and the FTC, which requires Facebook to establish and refine certain practices with respect to treatment of user data and privacy settings. The FTC settlement also requires bi-annual independent privacy audits. Facebook further discloses how the FTC and DPC audits have affected Facebook, and that Facebook expects to continue to be the subject of regulatory investigations and audits in the future by these and other regulators throughout the world.

- *Disclosure Tip:* When disclosing cybersecurity and privacy risks, companies should remember that vague statements about the possible risk of investigations are insufficient. To comply with the Division's guidance, companies should follow Facebook's lead and disclose specific details about prior and current investigations, as well as the risk of specific future investigations.

– Cybersecurity Risks

Facebook directly addresses the Cybersecurity Guidance in its disclosure regarding how computer malware, viruses, hacking, phishing attacks, and spamming could harm its business. Rather than just generally disclosing how cybersecurity risks can harm an internet business, Facebook takes the extra step and discusses exactly how cybersecurity risks affect it. The disclosure goes into detail about how Facebook's prominence makes it a target for cybersecurity risks. The disclosure further discusses the indirect consequences of cybersecurity risks, including how spammers may embarrass or annoy Facebook users and make Facebook less user-friendly.

- *Disclosure Tip:* In addition to simply acknowledging that hackers and viruses are risks, companies should explain specifically *how* these risks can affect their business. Facebook's disclosure demonstrates that discussions about both direct and indirect costs of cybersecurity risks are essential to providing adequate disclosure.

– Cybersecurity and Privacy Breaches

The unique nature of Facebook's business makes the risk of cybersecurity and privacy breaches even greater. In its Risk Factors, Facebook emphasizes how third-party platforms and websites that are integrated into Facebook increase the risk that user information may be improperly accessed or disclosed. Specifically, these third-parties may fail to adhere to adequate data security practices or fail to comply with Facebook's terms and policies. Facebook discusses the direct costs of improper access to its users' information, such as legal or regulatory action against Facebook, and the indirect costs of improper access to its users' information, such as reputational and brand damage.

- *Disclosure Tip:* As Facebook exemplifies, a company disclosing risks related to cybersecurity and privacy breaches should not only discuss risks regarding its internal user data policies and procedures, but should also disclose risks regarding external third-parties' use of user information and the risk of improper access to or disclosure of that information. Following the Cybersecurity Guidance, Facebook discusses the risks associated with outsourcing parts of its business, such as third-party integration into Facebook's website. Other companies should disclose how they allow third-parties to access user data, and how that relationship potentially creates additional cybersecurity and privacy related risks.

Aside from discussing the direct risks associated with cybersecurity and privacy breaches, Facebook also emphasizes the secondary risks related to unfavorable media coverage and negative user reaction to cybersecurity and privacy breaches. Specifically, Facebook explains that unfavorable media coverage or publicity regarding its privacy practices, regulatory activity, or the actions of platform developers could adversely affect Facebook's reputation and have an adverse effect on the size, engagement, and loyalty of Facebook's user base.

- *Disclosure Tip:* Companies that collect user data should disclose risks related to potential reputational damage and negative publicity that could result from cyber incidents. Doing so completes the picture regarding secondary and indirect risks of cybersecurity or privacy breaches. Providing investors with this breadth of disclosure will better ensure compliance with the Cybersecurity Guidance.

– **U.S. and Foreign Laws Relating To Privacy and Data Protection**

In its Risk Factors, Facebook recognizes the evolving landscape of privacy and data protection laws in the U.S. and abroad by disclosing how these changing laws have affected and will continue to affect its business. In addition to general statements about the impact of privacy and data protection regulations, the disclosure goes further and discusses potential changes to specific regulations (i.e., the 1995 European Union Data Protection Directive). Facebook discloses that these changes could delay or impede the development of new Facebook products, and could result in increased operational costs, negative publicity, fines, and litigation.

- *Disclosure Tip:* It is important for companies to tailor risk factors concerning government regulations to their specific industry and to specific regulations, rather than simply providing a vague description about how government regulations generally can cause risk. This provides potential investors with greater disclosure about actual risks related to new or changing regulations.

Business[4]

The Cybersecurity Guidance regarding disclosures in the "Description of the Business" section focuses primarily on the disclosure of cyber incidents that materially affect the Company's products, services, relationships with customers or suppliers, and competitive conditions. In the Business section of its S-1, Facebook's discussion of specific cyber incidents is minimal and relates primarily to its settlement with the FTC resolving its investigation into various practices with respect to Facebook's treatment of user data and privacy settings (as also discussed in Facebook's Risk Factors). Presumably, the FTC investigation is the only "cyber incident" that Facebook believes materially affects the areas listed above, and thus is the only cyber incident that Facebook was required to disclose.

- *Disclosure Tip:* Companies preparing cyber incident related disclosures in the "Description of the Business" section should disclose all cyber incidents that are *material*. Companies should disclose these incidents in the "Description of the Business" section even if they previously disclosed the incidents in "Risk Factors". This will ensure completeness and full compliance with the Cybersecurity Guidance in both relevant sections.

Follow the Roadmap – Find Your Data – Know Your Risks

By providing extensive disclosures related to cybersecurity, cyber incidents, and privacy risks, Facebook has given companies facing cybersecurity and privacy risks a roadmap on how to comply with the Cybersecurity Guidance. Although specific disclosures and disclosure language will differ from Facebook's S-1, companies should follow Facebook's lead regarding the framework, breadth, and detail of its disclosures.

The most important point that companies should take away from Facebook's S-1 disclosures is *specificity*. Boilerplate and generic disclosures related to cybersecurity and privacy risks are inadequate and discouraged by the SEC. To ensure full compliance with the Cybersecurity Guidance, companies should disclose risks specific to their business, while including details concerning how those risks may directly and indirectly affect the company's business. Key to a company's ability to provide adequate and fulsome disclosure in accordance with the expectations of the Cybersecurity Guidance, is a risk assessment related to data privacy and information security issues. Without that, even beginning to craft specific disclosure becomes an impossible task. If a company discloses material and specific information related to its cybersecurity and privacy risks and tailors those disclosures to its business as Facebook has done in its S-1, then it will be well on its way to providing adequate disclosure to investors and to minimizing the comments it receives from the SEC.

Cynthia J. Larose is a Member of Mintz Levin's Corporate & Securities Section, Chair of the Privacy & Security practice, and a Certified Information Privacy Professional (CIPP). Cynthia represents companies in information, communications, and technology, including e-commerce and other electronic transactions. She counsels clients through all stages of the "corporate lifecycle," from start-ups through mid- and later-stage financings to IPO, and has broad experience in technology and business law, including online contracting issues, licensing, domain name issues, software development, and complex outsourcing transactions. Cynthia has extensive experience in privacy, data security, and information management matters, as well as data transfers in the context of mergers and acquisitions and technology transactions. She conducts privacy audits and risk assessments to determine data and transaction flow and to assess privacy practices, and assists with drafting and implementation of privacy policies and information security policies and procedures and monitoring of privacy "best practices" across all levels of the enterprise.

Adam M. Veness is an Associate in the Corporate & Securities Section and is based in the firm's Boston office. He was a Summer Associate at Mintz Levin in 2009. Before rejoining Mintz Levin, Adam focused on general civil litigation, construction litigation, personal injury defense, and employment matters. His professional experience also includes clerking for the United States Army JAG Corps. During law school, Adam participated in the Civil Litigation Clinic through Greater Boston Legal Services where he represented clients in Social Security disability appeals and in unemployment insurance hearings.

[1] *See* Facebook, Inc., Registration Statement (Form S-1) at 11 (Feb. 1, 2012).

[2] *See* CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011).

[3] *See* Facebook Form S-1 at 11.

[4] *Id.* at 71.