BEST'S REVIEW
www.bestreview.com June 2015

A Closer Look

Increased cybersecurity regulations are impacting the insurance and financial technology sectors.

by Jennifer Chu, Marilyn Lion and Jim Pastore

From apps that allow policyholders to submit claims, to software that modernizes distribution of insurance products, insurance technology innovations are poised to grab a larger share of the booming financial technology market and present a wealth of opportunities for insurance companies and other investors.

Merger and acquisition activity in the fintech sector has made headlines in recent years with hundreds of deals announced in the past three years, including several multibillion-dollar acquisitions by private equity sponsors. At the same time, in the wake of cyberattacks on companies like Anthem and Premera Blue Cross, data privacy and cybersecurity have moved to the forefront of regulatory concerns for insurance companies and their service providers.

What does this increased regulatory focus mean for fintech? Some companies that face licensing requirements—like those conducting claims adjusting, brokerage, third party administrator or similar functions—will feel the impact directly through increased regulatory requirements.

Less obvious, though arguably equally important, is the impact that increased regulation can have on the fintech companies servicing the insurance industry. Regulators increasingly are focusing on the relationships that insurance companies maintain with their third-party providers, demanding that insurers regularly monitor third-party providers to ensure that they adequately safeguard sensitive consumer data. Given this increased regulatory scrutiny, understanding cybersecurity

Key Points

What Happened: Recent cyberattacks on insurers have increased regulatory attention.

Biggest Focus: The impact that increased regulation can have on the fintech companies servicing the insurance industry bears watching.

Going Forward: Fintech companies servicing insurance companies can expect to see more pointed questions about their own cybersecurity practices.

Contributors: **Marilyn Lion** is a partner in the Financial Institutions Group; **Jim Pastore** was elected partner effective July 1, 2015 in the Cybersecurity & Data Privacy practice and the Intellectual Property Litigation Group; and **Jennifer Chu** was elected partner effective July 1, 2015 in the Mergers & Acquisitions Group of Debevoise & Plimpton LLP. They can be reached at *fintech@debevoise.com*


Lion


Pastore


Chu

regulations in the insurance industry and their potential impact on business operations should be a consideration when investing in fintech.

Cybersecurity regulation in America consists of a patchwork of federal and state actors, as well as a variety of industry-specific bodies that produce best practices and other guidance. Insurance companies must navigate a 50-state mosaic of data protection and privacy laws. In the event of a breach, for example, they may find themselves combing through 47 different laws that determine whether, when and how companies must notify customers about data breaches. And new regulations and guidance are being issued frequently.

For example, the National Association of Insurance Commissioners identified cybersecurity as one of the organization's key initiatives for 2015, and established a Cybersecurity Task Force to provide guidance on, among other things, insurers'

Cyber-Diligence Considerations For Investments in Insurance Tech Companies

The increased regulatory scrutiny on third-party providers is significant not only for fintech companies, but also for those considering investing in them. Assessing the effect of, and compliance with, emerging cybersecurity regulatory regimes applicable to insurance companies should be a key area of legal due diligence for a prospective buyer of an insurance tech company. Potential investors should also evaluate whether an insurance tech target is adequately prepared to fend off cyberattacks in the future and whether the company has the tools and business plan to remain operational in a climate focused on preparedness.

In order to evaluate how prepared a target fintech company is for cyberbreaches, due diligence can include examining the credentials, responsibilities and reporting positions of IT security personnel; reviewing the results of any penetration testing (which involves hired, ethical hackers who try to hack a company's systems, thereby identifying the systems' vulnerabilities) performed by the target; and reviewing the target's "tabletop" drills (which involve the company rehearsing the necessary steps to take in event of a breach).

Another area of due diligence might consist of reviewing the target company's data security protocols and determining whether there have been prior data security breaches, what steps were taken to remediate these breaches and whether those steps were successful in preventing further breaches.

Due diligence sometimes also includes reviewing the procedures the target company may have in place for issuing usernames and passwords to outsiders and the procedures for accessing the target's IT systems. For example, does access require merely a username and password or does it require multifactor authentication, such as an additional method of verifying that the user is authorized to access the system? (This last point has been a particular area of focus for the New York State Department of Financial Services; DFS Superintendent Benjamin Lawsky has called single-factor authentication a practice that "should have been dead and buried many years ago.")

Potential buyers can also compare the target fintech company's cybersecurity profile to external standards (for example, the National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity and the SANS Institute Critical Security Controls for Effective Cyber Defense) and even look to the regulatory pronouncements like the DFS 308 letter and the NAIC principles, which provide insight into the regulators' views of best practices on cyber preparedness.

A potential investor also should consider performing due diligence on the target's compliance with relevant privacy regulations, including with respect to outsourced functions. This means careful review of contracts with third parties to fully understand the target company's indemnity exposure. Additionally, the target's insurance coverage should be carefully reviewed to determine whether there are any gaps in coverage for cybersecurity breaches. The time period of coverage is a particularly pressing issue, as many hackers breach a system and then lie in wait for months or years before taking advantage of the information obtained.

Risk Allocation in Insurance Tech M&A

The market for fintech targets remains a seller's market. While this continues to be the case, buyers will likely continue to see sellers commanding not just large valuation multiples but also seller-friendly deal terms, such as low indemnity caps (or in some cases, no indemnity at all). Buyers seeking unusual or off-market protections for cybersecurity risks, such as special indemnities, may negatively distinguish themselves in competitive situations. All of this puts additional pressure when considering investing in insurance tech on a thorough due diligence of cybersecurity-related risks that is attuned to the new nexus of cybersecurity concerns and insurance regulation.

The bottom line is that, with regulators increasingly scrutinizing the relationships that regulated entities have with their third-party providers, fintech companies, and those who invest in them, would do well to review their cybersecurity practices sooner than later in order to position themselves for success.

risk management practices. In April, the NAIC's Cybersecurity Task Force adopted Principles for Effective Cybersecurity. These 12 principles endorse a risk-based approach that considers the resources of the regulated entity; include statements on the importance of safeguarding customer data; and endorse a coordinated approach to cybersecurity among state insurance regulators, insurers, insurance producers and the federal government.

Third-Party Scrutiny

Significantly for those investing in fintech, the principles also demand that insurers and other regulated entities take steps to ensure that third parties and service providers have adequate controls in place to safeguard sensitive data. The NAIC's principles call on regulators to include this area in their examinations. The implication is clear: Those entities that are regulated must do more to mind those entities that are not, but that nonetheless hold or access sensitive customer data—and regulators will be asking tough questions about those relationships during examinations. That focus is a natural outgrowth of the fact that a number of recent, high-profile cybersecurity attacks have involved hackers' abuse of credentials issued to third-party vendors that had access to the companies' IT systems.

The National Association of Insurance Commissioners' Principles for Effective Cybersecurity demand that insurers and other regulated entities take steps to ensure that third parties and service providers have adequate controls in place to safeguard sensitive data.

Other regulators outside the insurance industry also have announced an increased focus on cybersecurity, expressing specific concerns about third-party vendors. The Securities and Exchange Commission published a report in February 2015 summarizing the results of its Cybersecurity Examination Initiative that reviewed the practices of broker/dealers and investment advisers. The SEC reported that while most firms had written security policies and conducted periodic risk assessments, fewer firms had adequate cybersecurity policies with respect to vendors and business partners that were authorized to access their networks.

In the insurance world, New York State Department of Financial Services Superintendent Benjamin Lawsky has repeatedly stated that cybersecurity is an important area of focus for DFS in the near term. The DFS began surveying insurance companies about cyber-preparedness in 2013, and in February 2015 released a report on cybersecurity in the insurance industry.

According to the report, while 95% of surveyed insurers believed they were adequately staffed with respect to information security, only 14% of CEOs received monthly briefings on information security and few insurance companies identified or discussed cybersecurity as a stand-alone material risk in their 2014 annual enterprise risk management reports. The report also specifically called out third-party providers, concluding that "[e]nsuring that each institution obtains the appropriate representations and warranties from its third-party service providers, for example, would be a solid step in bolstering the institution's own cybersecurity." Lawsky echoed these sentiments in a Feb. 25 speech at Columbia Law School, revealing that DFS is considering "mandating that our financial institutions receive robust representations and warranties from third-party vendors that those vendors have critical cybersecurity protections in place."

As a follow-up to its February report, the DFS issued a request in March to CEOs, general counsels and chief information officers of insurers, requesting reports on cybersecurity pursuant to the DFS' authority under Section 308 of the New York Insurance Law.

The "308 letter" requires insurers to complete a special comprehensive risk assessment questionnaire on cybersecurity, which expands on the 2013 survey in light of more recent cybersecurity concerns. Many of the 16 questions address vendor management and pointedly ask what companies are doing to vet and monitor their vendors; what requirements companies impose on third parties to notify them of breaches; and whether companies demand that their third-party providers maintain minimum cybersecurity standards.

Taken together, these regulations suggest that fintech companies servicing insurance companies can, at the very least, expect to see more pointed questions about their own cybersecurity practices from their customers, and can expect to be required to take on more of the risk should a breach occur that endangers the insurance company's customers. As a result, fintech companies would do well to keep abreast of these regulatory changes, as they may impact both the costs of doing business and the potential liabilities they are required to assume under contracts with insurance companies. BR