SQUIRE PATTON BOGGS

Insurance Company Charged with Violations of New York's Cybersecurity Regulation

US – July 2020

The New York Department of Financial Services filed its first enforcement action alleging violations of New York's cybersecurity regulation that led to a breach of sensitive customer information. The action provides insight and guidance into the DFS's enforcement priorities and a warning to other financial institutions.

Three years after the regulation went into effect, the New York Department of Financial Services ("DFS") filed its first formal charges against an insurance company for allegedly violating several provisions of the state's cybersecurity regulation ("the Regulation") (Part 500 of Title 23 of the New York Codes, Rules, and Regulations). The Regulation applies to entities regulated by the DFS such as banks, credit unions, insurance companies, insurance agents, health maintenance organizations, money transmitters, mortgage companies, check cashers, and premium finance companies. DFS alleged five distinct violations, including failure to identify and remediate certain risks, thereby enabling the potential exposure of millions of mortgage-related documents that contained sensitive non-public personal information ("NPI"). According to the Statement of Charges and Notice of Hearing ("Statement of Charges"), the information included social security numbers, driver license images, bank account numbers, mortgage and tax records, and wire transfer receipts. A hearing is scheduled for October.

The charges brought by DFS are fair warning to any insurance company or financial institution that adopting controls that facially meet the Regulation are insufficient unless they actually reflect the results of a meaningful risk assessment and any deficiencies that arise are addressed promptly. In other words, business and information security teams must work together to assess and remediate risks, and management must respond when deficiencies and risks are identified. While the DFS may be the first state to bring an enforcement action against an insurance company, 11 other states have adopted very similar requirements for insurance companies. That number will increase as states continue to adopt the National Association of Insurance Commissioners' Insurance Data Security Model Act.

DFS implied that the Company missed several opportunities to fix the vulnerability that ultimately permitted exposure of NPI. In this case, the vulnerability stemmed from the Company's use of a document sharing system that permitted document access simply by sharing a URL without any additional log-in or authentication. The URL contained the actual document ID and thus other documents could be viewed simply by changing the number in the URL. The URLs shared via the document delivery system did not expire.

Although the Company's policies supposedly required employees to manually tag documents that contain NPI to prevent such documents from being shared, DFS alleged that many documents were not tagged. According to DFS, that meant that, over a period of a few years more than 850 million documents may have been accessible to anyone who had a URL address for a single document.

DFS began an investigation when the company reported the incident as required by the Regulation. The Company apparently reported the incident after being informed by a reporter that he was able to view highly sensitive consumer data, including social security numbers and drivers' licenses.

DFS found fault with the Company's actions on several fronts, starting with a lack of follow up when the vulnerability was initially reported by the cyber defense team. According to DFS, the Company became aware that documents were not correctly tagged as containing NPI (and thus excluded from sharing via the URL tool) and that documents had been subjected to Google search engine indexing and, yet, failed to correct the problem for several months. DFS identified several errors along the way, including misclassification of the severity of the problem, a mistaken belief that the document delivery system could not transmit NPI, the CISO's belief that accessible data was all publicly available and was not NPI, the cyber team's decision to conduct a minimal review of exposed documents (a sample of ten documents out of millions, none of the ten apparently contained NPI), a failure to follow the Company's own procedures, and a lack of accountability. The errors were allegedly compounded by management's decision not to implement certain recommended modifications and additional controls.

The Statement of Charges alleges five specific violations including (1) failure to conduct a risk assessment of the document storage and delivery systems despite the fact NPI was stored and transmitted on those systems; (2) lack of reasonable access controls; (3) failure to maintain and implement suitable data governance and classification policies for NPI; (4) a risk assessment that was insufficient to inform the design of a cybersecurity program because it failed to identify where in the system NPI was stored and transmitted; (5) inadequate cybersecurity awareness training for employees and affiliated agents, which was important because the process of correctly identifying NPI and preventing it from being transmitted depended solely upon employees and agents.

The enforcement action underscores the need for comprehensive risk assessments that include the participation of business units familiar with how systems are used and what information is in them. The warning for senior management and boards of directors is that reported vulnerabilities need to be taken seriously, business personnel need to be involved in the response, and, importantly, there must be accountability and responsibility for addressing vulnerabilities and recommendations. Of particular interest to the insurance industry is the implicit position of DFS that an insurance company's cybersecurity awareness training may need to include agents that have access to the company's systems. There are many lessons that can be learned from the allegations in this case.

Contacts

Susan T. Stead
Of Counsel, Columbus
T +1 614 365 2708
E sue.stead@squirepb.com

Elliot R. Golding
Partner, Washington
Data Privacy and Cybersecurity
T +1 202 457 6407
E elliot.golding@squirepb.com