Katten

PRIVACY, DATA AND CYBERSECURITY ADVISORY

The Wait is Over: New York Department of Financial Services Files First Enforcement Action Under Cybersecurity Regulation

August 7, 2020

KEY POINTS

- For the first time, New York's top banking and insurance regulator filed an enforcement action under the New York State Department of Financial Services (DFS) Cybersecurity Regulation (the Regulation).
- DFS' statement of charges against First American Title Insurance Company outlines some DFS enforcement considerations and enforcement, which had exposed tens of millions of records of consumers' sensitive personal information.

For the first time under the New York State Department of Financial Services' (DFS) Cybersecurity Regulation (23 NYCRR Part 500) (the Regulation), New York's top banking and insurance regulator filed an enforcement action in connection with a data breach.

On July 21, DFS filed a statement of charges against First American Title Insurance Company (First American) in connection with the exposure of tens of millions of records that contained consumers' sensitive personal information, including bank account numbers, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers' license images (Nonpublic Information or NPI).

What is the Cybersecurity Regulation and when does it apply?

DFS implemented the Regulation to standardize how covered institutions must structure their cybersecurity programs to protect NPI and to establish requirements, such as conducting regular risk assessments,[1] designating a Chief Information Security Officer (CISO),[2] implementing an incident response plan[3] and providing timely notification of incidents.[4] Subject to certain exemptions, a "covered entity" is any organization operating under, or required to operate under, a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.[5]

1 § 500.09
2 § 500.04
3 § 500.16
4 § 500.17
5 § 500.01(c)

As DFS issued the Regulation pursuant to section 408 of the Financial Services Law, each violation carries a civil monetary penalty of up to $1,000. While there has been some uncertainty surrounding what might constitute a violation of the Regulation, and how many violations might arise out of a single cyber incident, in its press release announcing the action against First American, DFS alleges that each instance of NPI encompassed within the statement of charges against First American constitutes a separate violation.

Why did DFS charge First American?

According to DFS, a vulnerability introduced during a software update to First American's document-management system in October 2014 allowed anyone with a web browser to view sensitive files without a password or other security measures. The exposure remained undetected until December 2018, when an internal penetration test discovered the vulnerability, which First American allegedly failed to remediate until May 2019. DFS alleges that "this lapse was caused by a cascade of errors that occurred substantially due to flaws in [First American's] vulnerability remediation program," including:

- First American's failure to follow its own cybersecurity policies, neglecting to conduct a security overview and a risk assessment of the document management system and the sensitive data associated with the vulnerability;
- First American misclassifying the vulnerability as "low severity" despite the magnitude of the document exposure, while also failing to investigate the vulnerability of that severity level within the 90 day timeframe as dictated by its internal cybersecurity policies;
- First American's failure to conduct a reasonable investigation into the scope and cause of the exposure, reviewing only a small handful of the millions of documents that were exposed, thus underestimating the seriousness of the vulnerability; and
- First American's failure to follow the recommendations of its internal cybersecurity team to further investigate the vulnerability and determine if sensitive documents were exposed.

What sections of the Regulation does DFS allege were violated?

According to the statement of charges, DFS alleges that First American violated six provisions of the Regulation:

- § 500.02: The requirement to maintain a cybersecurity program that is designed to protect the confidentiality, integrity and availability of the covered entity's information systems and which is based on the covered entity's risk assessment.
- § 500.03: The requirement to maintain a written policy or policies, approved by senior management, setting forth the covered entity's policies and procedures for the protection of its information systems and the NPI stored on those systems.
- § 500.07: The requirement to limit user access privileges to information systems that provide access to NPI and periodically review such access privileges.
- § 500.09: The requirement to conduct a periodic risk assessment of the covered entity's information systems to inform the design of its cybersecurity program.
- § 500.14(b): The requirement to provide regular cybersecurity awareness training for all personnel as part of the covered entity's cybersecurity program, and to update such training to reflect risks identified by the covered entity in its risk assessment.
- § 500.15: The requirement to implement controls, including encryption, to protect NPI held or transmitted by the covered entity both in transit over external networks and at rest.

What's next for DFS?

Upon taking over at DFS in June 2019, Superintendent Linda Lacewell assured that the agency would shift its enforcement policy to emphasize consumer protection.[6] Given the volume of the records, length of exposure and sensitivity of the NPI involved in the breach, there is a reasonable risk of the compromised data being exploited by bad actors to target companies and their employees in social engineering phishing attacks and Business Email Compromise (BEC) scams. In the real estate and financial services industries, BECs are among the most common cause of data breaches, with cyber criminals impersonating real estate agents, lenders, closing agencies or title and escrow firms to induce buyers into wiring funds to a fraudulent bank account.

With an administrative hearing scheduled for October 26, the charges against First American serve as an important reminder for covered entities to regularly review and assess whether their existing cybersecurity program complies with the Regulation, and if any risks or vulnerabilities are identified, document a corrective action plan to address such items. Katten's Privacy, Data and Cybersecurity and Financial Markets and Funds groups continue to monitor DFS' enforcement of the Regulation and are standing by to advise covered entities on their cybersecurity frameworks and mitigating regulatory risk.

---

[6] https://www.law.com/newyorklawjournal/2019/09/03/dfs-enforcement-to-increase-focus-on-consumer-protection-where-cfpb-steps-down-dfs-has-to-step-up/?slreturn=20200003105955 (Sept. 3, 2019).

CONTACTS

For more information, please contact Katten's Privacy, Data and Cybersecurity or Financial Markets and Funds practices, or any of the following attorneys:

Doron Goldstein
+1.212.940.8840
doron.goldstein@katten.com

Susan Light
+1.212.940.8599
susan.light@katten.com

Jeremy Merkel
+1.212.940.6339
jeremy.merkel@katten.com