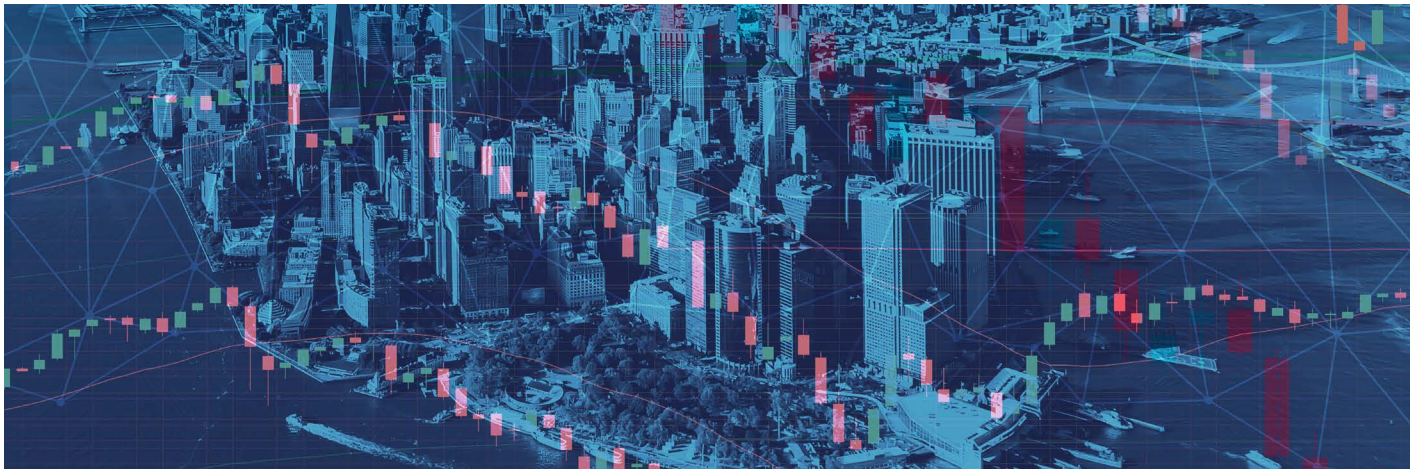
WFG National Title

SAFE Alert!

NY Cybersecurity Breach Violation will cost lender $1.5M



March 2021

A lender, based out of Maine, has agreed to pay a $1.5 million fine for violating several provisions of New York's cybersecurity regulations after an employee's email account was compromised as the result of a phishing attack in 2019. Even though the employee collected sensitive consumer data from loan applicants, the breach was never fully investigated nor reported.

Although Multi-factor authentication (MFA) had been implemented for email, the targeted employee had approved the required MFA authorization request on her cell phone on four separate occasions, even though she was not attempting to access her email account at the time. The next day, when the fifth request for authorization came in, she notified her company and access to her email was blocked. IT verified that unauthorized access happened four times from an IP address in South Africa and involved just her email account, but no further investigation was done and no cyber breach was reported.

The New York State Department of Financial Services (DFS) stated that Residential Mortgage Services Inc. failed to:

- investigate whether an attacker, who compromised a single email mailbox, accessed private data of individuals.
- satisfy various state breach notification obligations.
- notify the DFS of the incident.
- conduct a cybersecurity risk assessment.

"This failure was especially egregious given Employee's daily handling of the private data of mortgage loan consumers, including social security numbers and bank account numbers, via her breached email account," the DFS said. Once prompted by the DFS last year, the lender cooperated with the investigation, which also found they did not have a comprehensive cybersecurity risk assessment performed per the cybersecurity regulation.

In 2017, DFS implemented regulations setting out how financial services companies licensed to operate in New York should construct their cybersecurity programs. The rules include regular risk assessments, timely notifications of incidents, and ensuring that companies limit access to sensitive customer information.