THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 34 No. 12 December 2018

CYBER-SECURITY INSURANCE ISSUES IN MORTGAGE LENDING

With cyber-attacks on the rise, mortgage lenders in particular need to bolster their cyber-security planning with insurance. The author calls attention to common provisions of cyber-specific insurance policies and the coverage for cyber-events by traditional business policies. She concludes with a review of steps an insured must take to secure coverage after a cyber-event.

By Leslie C. Thorne *

Major data breaches make headlines on a near-weekly basis. These attacks are increasing in size and frequency for a number of reasons, but it all boils down to this: companies' and individuals' confidential data is valuable to hackers. Law, accounting, and financial firms have traditionally been high-value targets because they hold a large amount of sensitive client data. Mortgage lenders can be particularly vulnerable because large numbers of third parties transfer data in connection with the mortgage lending process. They can be particularly attractive to cyber-criminals because they possess more specific and comprehensive financial data on any given individual than almost any other single entity. To mitigate the risk and effect of cyber-attacks, lenders should take steps to prevent data breaches and mitigate the damage if one does occur. Because financial institutions and regulatory agencies have been on the forefront of cyber- security, the models and guidelines provided in that sector are helpful to any institution looking to develop or bolster its cyber-security planning.

Key to a mortgage lender's ability to protect itself is insurance. In addition to the direct financial losses a mortgage lender may itself face as a result of a breach or attack, it can also face catastrophic claims from all quarters: clients, shareholders, other banks, regulators, etc.

CYBER-SPECIFIC INSURANCE POLICIES

Losses stemming from claims and litigation after a breach can be substantial and go on for years. But insurance — and cyber-coverage in particular — allows lenders to shift a broad array of the attendant costs. Depending on the policy, cyber-insurance may comprehensively cover the wide range of losses causes by a breach: (1) forensic investigation and system restoration costs; (2) defense and indemnity costs associated with litigation resulting from the loss of personal information or other sensitive data; (3) defense costs and penalties associated with regulatory investigations; (4) notification costs and credit monitoring for affected customers and employees; (5) losses attributable to the theft of the policyholder-company's own data (including transfer of funds); (6) business interruption costs attributable to a cyber-attack; (7) costs required to investigate threats of cyber-extortion and payments to extortionists; and (8) crisis

* *LESLIE C. THORNE is a partner in the Austin office of Haynes and Boone, LLP. Her e-mail address is leslie.thorne@haynesboone.com.*