Statement by FDIC Chairman Jelena McWilliams on the Notice of Proposed Rulemaking on Computer-Security Incident Notification at the FDIC Board Meeting

Last Updated: December 15, 2020

Technology has played a transformative role in the financial services industry. Banks rely on technology to manage their operations, interact with customers, and develop new products and services. As Chairman, one of my top priorities has been to foster innovation at our Nation's banks. For many banks, that includes removing unnecessary regulatory impediments and reducing operational uncertainty too often associated with third-party technology partnerships.

While technology provides undeniable benefits, banks must also take steps to manage the risk that accompanies new technologies, to protect the sensitive information in their systems, and to ensure resilience in the face of attacks from those that might seek to disrupt bank operations.

As the FDIC noted in January 2020, "disruptive and destructive attacks against financial institutions have increased in frequency and severity."[1] Cyber attackers have used numerous tools to obtain access to financial institution systems and networks, from the use of stolen credentials and phishing to more destructive ransomware attacks that could compromise data or render systems unusable.[2]

While some computer-security incidents must be reported as a Suspicious Activity Report (SAR) or under Gramm-Leach-Bliley, these reports may not be filed with regulatory agencies in time to provide assistance to an affected bank or to coordinate a regulatory or security response to a cyberattack that may affect multiple institutions.

The notification requirements included in this proposed rulemaking would address this gap in timely regulatory awareness of the most significant computer-security incidents affecting banking organizations.

Under the proposed rule, a banking organization would be required to notify its primary federal regulator of any significant computer-security incident that may "materially disrupt, degrade, or impair" the bank's operations or may threaten the financial stability of the United States. This notification would be required within 36 hours of the time that a bank develops a "good faith belief" that such an incident has occurred. A bank service company would have an obligation to report to affected bank customers any incident that could disrupt, degrade, or impair the services provided to the bank for four or more hours.

The notice required by the rule does not include a formal, comprehensive assessment of the incident or the scope of the harm. For example, an FDIC-supervised bank would merely be required to send an email or call a designated point of contact at the FDIC and make them aware of the incident.

Moreover, not every computer-security incident must be reported. Only those that meet the high standard of a "notification incident" must be reported. Based on a review of supervisory data and SARs, the FDIC, Office of the Comptroller of the Currency (OCC), and Federal Reserve estimate that only about 150 incidents occur annually that would meet the significant standard for a notification incident.

The rule proposed by the agencies today provides appropriate balance – avoiding unnecessarily difficult or time-consuming reporting obligations while ensuring that regulatory agencies are in a position to provide assistance to a bank or the broader financial system when significant computer-security incidents occur.

Given the increasing cyber threat facing our banks, I support this proposal and look forward to reviewing industry comments as we work to close this gap in our oversight of the financial system.

I would like to thank our team, as well as the teams at the Federal Reserve and the OCC, for a collaborative effort to prepare a thoughtful and balanced proposal.

---

[1]*See* FDIC, FIL-03-2020, *Heightened Cybersecurity Risk Considerations* (Jan. 16, 2020), available at https://www.fdic.gov/news/financial-institution-letters/2020/fil20003.html.

[2]*See* id.