Date Published 22 November 2021 by Jimmie Franklin

Cybersecurity Rules Tightened For U.S. Banks

The three federal US financial regulators have issued a new cyber rule for banks - meaning that they need to report cyber incidents within 36 hours.

Banks in the US have a new compliance burden coming their way in May due to a new rule written up by the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency.

The approval of this rule has been undertaken with the intention of improving information sharing about cyber incidents that may affect the US' banking system.

Banking organisations will now be required to notify their primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organisation determines that a cyber incident has occurred.

Financial institutions in the US were already subject to a degree of compliance in this area, for example, under the Bank Secrecy Act as well as the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

However, according to David F. Katz, a partner at Adams and Reese, this does not cover all cybersecurity incidents. "Currently, these standards do not include all computer-security incidents of which the agencies, as supervisors, need to be alerted and would not always result in timely notification to the agencies," he said, pointing out that the new rules will help change this.

According to the document released by the agencies, this new requirement will help promote early awareness of emerging threats to banking organisations and the broader financial system, ensuring they, "react to these threats before they become systemic."

The rule was backed by a majority of respondents when it was out for consultation, with people supporting the need for prompt notice of significant cyber incidents.

And this is part of the reason why cyber experts believe these new requirements may not end up being difficult to comply with.

"The final rule incorporated industry recommendations and won't overly burden financial institutions," said Kurt Suhs, Chief Executive Officer at Cyber Special Ops.

This new rule will help banking regulators address cyber threats before they become systemic, according to Suhs. "Certainly, a systemic cyberattack against critical infrastructure such as the

financial services sector could have a devastating impact on consumers.”

Yet, the regulation does not cover all relevant areas.

“What the Final Rule doesn’t address is the impact of a cyberattack against the financial institution’s commercial and consumer borrowers resulting in loan delinquency, charge offs or, in the worst-case scenario, insolvency of the financial institution,” he said.

Notification is required for incidents that have materially affected or are deemed reasonably likely to materially affect, the viability of a banking organisation's operations, its ability to deliver banking products and services, or the stability of the financial sector.

Once in effect, the new rule will also require a bank service provider to notify affected customers as soon as possible when the provider determines that it has experienced a cybersecurity incident that has materially affected or is reasonably likely to materially affect the bank’s customers for four or more hours.

Jurisdictions

United States

Authorities

Federal Deposit Insurance Corporation - US

Federal Reserve

Specialisms

Customer Protection

Cybersecurity

Products And Services

Bank Accounts