

# FDIC Advisory Committee on Community Banking

November 3, 2021

Information Technology Supervision Update



# Cybersecurity – FinCEN Ransomware Report

This report is issued pursuant to Section 6206 of the Anti-Money Laundering Act of 2020 which requires the Financial Crimes Enforcement Network to periodically publish threat pattern and trend information derived from financial institutions' Suspicious Activity Reports.



[Published October 15, 2021](#)

**FDIC**

# Cybersecurity – FFIEC Authentication Guidance Update

- Scope:
  - business & consumer customers
  - **employees**
  - **3<sup>rd</sup> parties – people & computers**
- “... malicious activity resulting in compromise of customer and user accounts and information system security has shown that **single-factor authentication**, either alone or in combination with layered security, **is inadequate** in many situations.”

Federal Financial Institutions Examination Council



3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

## Authentication and Access to Financial Institution Services and Systems

### Introduction

The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members<sup>1</sup> is issuing this guidance titled *Authentication and Access to Financial Institution Services and Systems* (the Guidance) to provide financial institutions with examples of effective risk management principles and practices for access and authentication. These principles and practices address business and consumer customers, employees, and third parties that access digital banking services<sup>2</sup> and financial institution information systems.

The Guidance replaces the FFIEC-issued *Authentication in an Internet Banking Environment (2005)* and the *Supplement to Authentication in an Internet Banking Environment (2011)*, which provided risk management practices for financial institutions offering Internet-based products and services. This Guidance acknowledges significant risks associated with the cybersecurity threat landscape that reinforce the need for financial institutions to effectively authenticate users and customers<sup>3</sup> to protect information systems, accounts, and data. The Guidance also recognizes that authentication considerations have extended beyond customers and include employees, third parties, and system-to-system communications.

This Guidance highlights risk management practices that support oversight of identification, authentication, and access solutions as part of an institution's information security program. Periodic risk assessments inform financial institution management's decisions about authentication solutions and other controls that are deployed to mitigate identified risks. When a risk assessment indicates that single-factor authentication with layered security is inadequate, multi-factor authentication (MFA) or controls of equivalent strength, combined with other layered security controls, can more effectively mitigate risks associated with authentication.

Financial institutions are subject to various safety and soundness standards, such as the standard to have internal controls and information systems that are appropriate to the institution's size and complexity and the nature, scope, and risk of its activities.<sup>4</sup> Applying the principles and

<sup>1</sup> The Council has six voting members: a member of the Board of Governors of the Federal Reserve System, the Chairman of the Federal Deposit Insurance Corporation; the Chairman of the National Credit Union Administration; the Comptroller of the Currency of the Office of the Comptroller of the Currency; the Director of the Consumer Financial Protection Bureau; and the Chairman of the State Liaison Committee.  
<sup>2</sup> Digital banking refers to any banking service or platform that utilizes Internet or mobile cellular network communications for providing customers with banking services or transactions.  
<sup>3</sup> For purposes of this Guidance only, the terms "users" and "customers" are defined in section 1 of this Guidance.  
<sup>4</sup> See, for example, Interagency Guidelines Establishing Standards for Safety and Soundness: 12 CFR 30, Appendix A, II(A) (OCC); 12 CFR 208, Appendix D-1, II(A) (FRB); and 12 CFR 364, Appendix A, II(A) (FDIC). See also 12 CFR § 741.3 (NCUA).

1

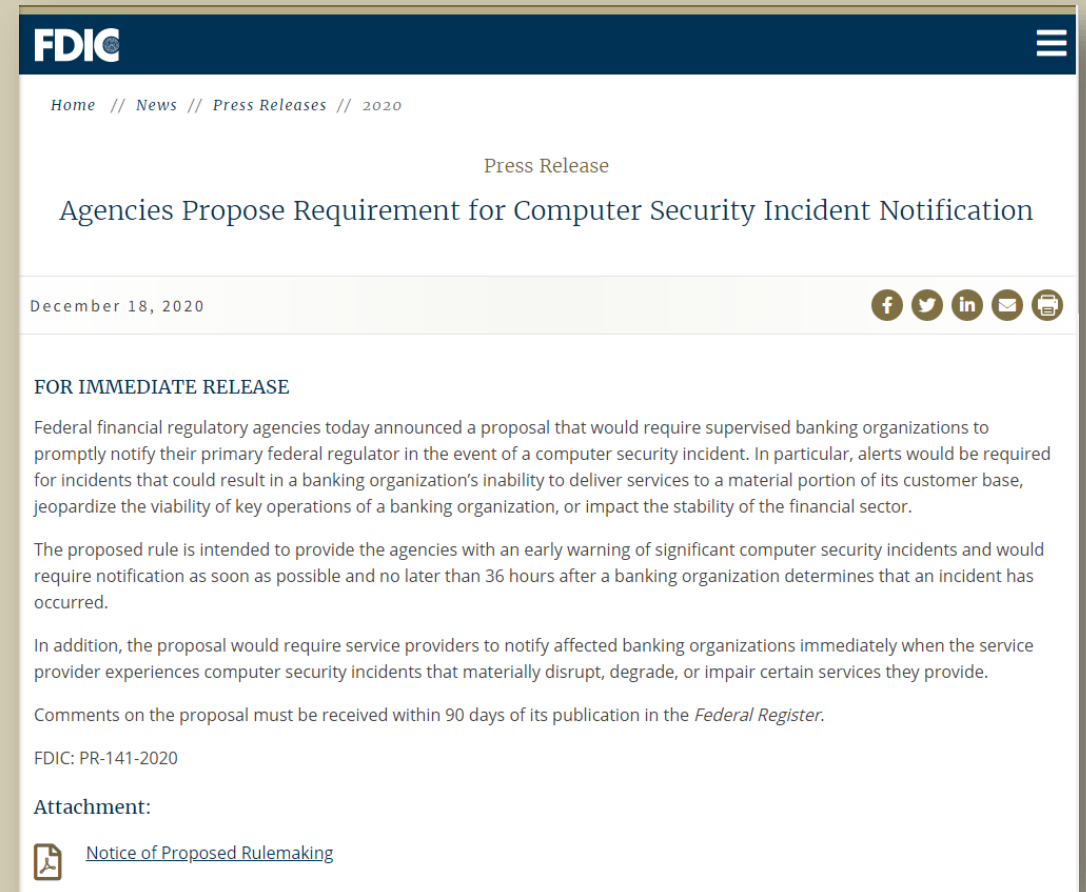
Published August 11, 2021



# Cybersecurity – Computer Security Incident Notification

## Major Themes From the Comments

- Focus on critical computer-security problems – avoid insignificant matters
- Simplify reporting to banks and to regulators
- Banks and service providers may need more time to determine that notification is required
- Existing contracts typically contain notification requirements
- Statutes and regulations require notification to regulators (e.g., SARs, GLBA)



The screenshot shows the FDIC website's press release page. At the top is the FDIC logo and a navigation menu. Below the logo is a breadcrumb trail: Home // News // Press Releases // 2020. The main heading is 'Press Release' followed by the title 'Agencies Propose Requirement for Computer Security Incident Notification'. The date 'December 18, 2020' is displayed on the left, and social media icons for Facebook, Twitter, LinkedIn, Email, and Print are on the right. The body of the release begins with 'FOR IMMEDIATE RELEASE' and states that federal financial regulatory agencies have announced a proposal to require supervised banking organizations to promptly notify their primary federal regulator in the event of a computer security incident. It further details that alerts would be required for incidents that could result in a banking organization's inability to deliver services to a material portion of its customer base, jeopardize the viability of key operations, or impact the stability of the financial sector. The proposed rule is intended to provide an early warning of significant incidents and requires notification within 36 hours. It also notes that service providers must notify affected banking organizations immediately when their services are materially disrupted. Comments on the proposal must be received within 90 days of publication in the Federal Register. The release ID is FDIC: PR-141-2020. An attachment link is provided for the 'Notice of Proposed Rulemaking'.

[Published December 18, 2020](#)