FDIC Advisory Committee of State Regulators

October 6, 2021

State-Federal Coordination

FDIC
FEDERAL DEPOSIT INSURANCE CORPORATION

Cybersecurity – FFIEC Authentication Guidance Update

- Scope:
  - business & consumer customers
  - ***employees***
  - ***3rd 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[1] 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[2] 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[3] 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.[4] Applying the principles and

[1] 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.
[2] 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.
[3] For purposes of this Guidance only, the terms "users" and "customers" are defined in section 1 of this Guidance.
[4] 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

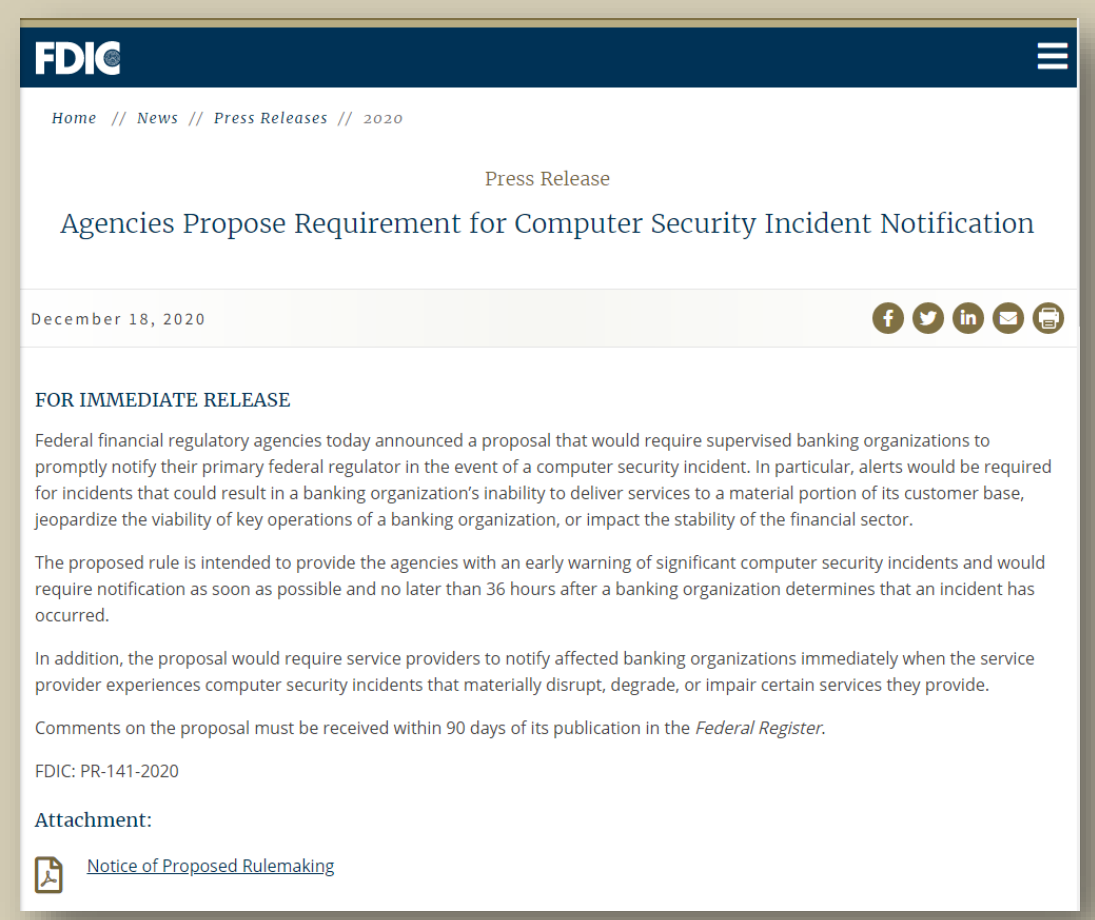
[Published August 11, 2021]

FDIC

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)



FDIC

Home // News // Press Releases // 2020

Press Release

Agencies Propose Requirement for Computer Security Incident Notification

December 18, 2020

FOR IMMEDIATE RELEASE

Federal financial regulatory agencies today announced a proposal that would require supervised banking organizations to promptly notify their primary federal regulator in the event of a computer security incident. In particular, 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 of a banking organization, or impact the stability of the financial sector.

The proposed rule is intended to provide the agencies with an early warning of significant computer security incidents and would require notification as soon as possible and no later than 36 hours after a banking organization determines that an incident has occurred.

In addition, the proposal would require service providers to notify affected banking organizations immediately when the service provider experiences computer security incidents that materially disrupt, degrade, or impair certain services they provide.

Comments on the proposal must be received within 90 days of its publication in the *Federal Register*.

FDIC: PR-141-2020

Attachment:

Notice of Proposed Rulemaking

Published December 18, 2020

FDIC

AML Act § 6101: National Anti-Money Laundering and Countering the Financing of Terrorism Priorities

National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Priorities were issued by the Financial Crimes Enforcement Network (FinCEN) on June 30, 2021, and include:

- Corruption
- Cybercrime
- Terrorist Financing
- Fraud
- Transnational Criminal Organizations
- Drug Trafficking Organizations
- Human Trafficking and Smuggling
- Proliferation Financing

FDIC

AML Act § 6101 – Rulemaking

FinCEN will amend AML Compliance Program Rules

- Incorporating the AML/CFT Priorities and other updates
- Issuing a notice of proposed rulemaking for public comment

The FDIC plans to amend the Bank Secrecy Act (BSA) Compliance Program Rule

- Conforming changes to FinCEN's AML Compliance Program Rules
- Ensuring consistency in the requirements

FDIC

§ 6403 – Corporate Transparency Act

- Reporting companies will be required to report beneficial ownership information to FinCEN.
- FinCEN will issue regulations implementing the beneficial ownership information reporting requirements.
- FinCEN's customer due diligence (CDD) requirements will be revised within one year of the effective date of those reporting requirements.
- Until those changes are made, banks are required to identify and verify beneficial owners of legal entity customers.

FDIC

Federal Financial Institutions Examination Council Considerations

AML Act §6209 – Testing Methods Rulemaking

- Required rulemaking to establish standards by which financial institutions are to test the technology and related technology internal processes to facilitate compliance with BSA requirements.

AML Act §6216 – Review of Regulations and Guidance

- In consultation with the FFIEC and other stakeholders, the U.S. Department of the Treasury will conduct a formal review of the regulations implementing the BSA and related guidance.

AML Act § 6307 – Annual AML/CFT Examiner Training

- In consultation with the FFIEC and other stakeholders, the U.S. Department of the Treasury will establish appropriate training materials and standards for use in the training.

Relevant FFIEC BSA/AML Examination Manual Updates

- Manual updates will incorporate implemented sections of the AML Act, emphasize the risk-focused approach and spectrum of risks, and differentiate legal requirements from examiner instructions.

FDIC