On August 11, the Federal Financial Institutions Examinations Council (FFIEC) issued new guidance, providing examples of effective authentication and access risk management principles and practices for financial institutions. The principles and practices relate to access to digital banking services and information systems by customers, employees, and third parties accessing digital banking services and financial institution information systems. The FFIEC — whose voting members include representatives from the FDIC, the NCUA, the OCC, the CFPB, the Federal Reserve Board, and the State Liaison Committee — issued the guidance as an update to prior submissions from 2005 and 2011.

Among other things, the guidance:
• Highlights the current cybersecurity threat environment including increased remote access by customers and users, and attacks that leverage compromised credentials; and mentions the risks arising from push payment capabilities.

• Recognizes the importance of the financial institution’s risk assessment to determine appropriate access and authentication practices to determine the wide range of users accessing financial institution systems and services.

• Supports a financial institution’s adoption of layered security and underscores weaknesses in single-factor authentication.

• Discusses how multi-factor authentication or controls of equivalent strength can more effectively mitigate risks.

• Includes examples of authentication controls, and a list of government and industry resources and references to assist financial institutions with authentication and access management.

According to the FFIEC, the guidance is meant as neither an endorsement nor a “comprehensive framework” for any specific information security identity and access program, and is intended to apply not only to financial institutions, but also to any third-party acting on behalf of a financial institution that provides the accessed information systems and authentication controls.

**Putting It Into Practice:** Financial institutions and their third-parties would be well-served to review their controls and procedures, including risk management practices that support oversight of identification and authentication, how to periodically evaluate the effectiveness of user and customer authentication controls, and what processes are in place to monitor, log, and report activities to identify and track unauthorized access.

Copyright © 2021, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume XI, Number 238

**Source URL:** https://www.natlawreview.com/article/ffiec-issues-updated-guidance-authentication-and-access-to-financial-institution