Articles + Publications | September 3, 2021

FFIEC Guidance Emphasizes the Key Role of Risk Assessments in Supporting Strong Financial Institution Authentication and Access Controls

WRITTEN BY

Shannon VanVleet Patterson | James W. Stevens | Alyson P. Tseng

Featured in the September Virginia Association Community Banks Newsletter.

As our colleagues from the Consumer Financial Services Group reported on August 11, the Federal Financial Institutions Examination Council (FFIEC) issued guidance titled "Authentication and Access to Financial Institution Services and Systems." The guidance updates and replaces prior FFIEC guidance, and provides financial institutions with examples of effective risk management principles and practices for access and authentication. The guidance underscores the need for financial institutions to extend access and authentication considerations beyond consumer and business customers to include employees, particularly security administrators and senior management, and third parties, such as cloud service providers and other vendors.

Financial institutions face significant cybersecurity risks. Driven by the convenience of mobile banking on multiple devices, the expansion of digital banking services and information system access points has provided attackers with more opportunities to obtain unauthorized access to or exfiltrate data, exposing information and credentials of customers, employees and third parties. Attacks have become increasingly sophisticated, demonstrating a need for stronger authentication and access controls for financial institutions.

A central theme of the guidance is the importance of risk assessments in supporting decisions regarding authentication techniques and access management practices. Financial institutions should engage in targeted risk assessments before launching new financial products or services to evaluate potential vulnerabilities and plan for appropriate authentication and access controls. In addition, periodic enterprise-wide risk assessments that include input from a variety of business functions, such as fraud research, customer service, and cybersecurity personnel, help ensure that financial institutions are identifying and addressing current risks and implementing appropriate controls. An effective risk assessment that focuses on customer transactions that present increased risk of financial loss or potential breach of information; on users with remote access to critical financial institution systems or data; or on risks arising from digital payment services that have shorter processing windows, push-payment capabilities, and limited fraud management functionality, can identify areas where enhanced authentication controls such as multifactor authentication may be most valuable to mitigate risk.

As the guidance indicates, robust and timely risk assessments continue to serve an integral role in financial institutions' ability to maintain safety and soundness, navigate business demands, and satisfy increasing customer desire for reliable and secure digital banking services in a shifting cybersecurity landscape.

RELATED INDUSTRIES + PRACTICES

- Financial Services
- Payments + Financial Technology