Alert

September 14, 2021

COZEN O'CONNOR

FFIEC Updates Guidance to Financial Institutions for Authentication and Access

The Federal Financial Institutions Examination Council (FFIEC), an interagency body of leading financial regulators, including the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, recently issued updated guidance to financial institutions on recommended best practices for information system authentication and access management controls. Titled *Authentication and Access to Financial Institution Services and Systems* (available here), it replaces previous FFIEC guidance, *Authentication in an Internet Banking Environment* (2005) and *Supplement to Authentication in an Internet Banking Environment* (2011).

The 2005 guidance focused exclusively on customer authentication to online banking systems. It emphasized that financial institutions should use authentication methods that are commensurate with the risks associated with the products and services offered. It also stated that the regulators did not consider single factor authentication to be adequate for high risk transactions, which it described as transactions involving access to customer information or the movement of funds to other parties. The 2005 guidance also provided that financial institutions should adjust their controls based on their periodic risk assessments.

The 2011 guidance was intended to update and amplify specific areas of the 2005 guidance, such as risk assessments and layered security. Additionally, it established minimum control expectations and identified certain controls that were recognized as less effective. Furthermore, the 2011 guidance identified most uses of online banking as high risk because the online banking transactions generally involved access to account information, payment systems, and interbank funds transfers. For consumer customers, the 2011 guidance recommended layered authentication controls. Layered security is the use of different controls, such as authentication controls, at different points in a system or a transaction so that a weakness in one control is compensated for by a different control. However, for business customers, it recommended multifactor authentication in addition to other layered authentication controls.

The 2021 guidance represents the next step in the regulators' approach to the topic as the threat environment and IT and security systems have evolved. The new guidance addresses authentication in three main areas. First, as with the previous guidance, it discusses both business and personal customers using online banking systems. But the new guidance expands its reach to users, such as employees, board members, and service providers, accessing a financial institution's internal IT systems. Additionally, the 2021 guidance addresses authentication of service accounts, applications, and devices on a financial institution's network.

The new guidance takes a more nuanced approach to high risk situations. The earlier guidance focused on high risk transactions, which were transactions involving access to customer information or the movement of funds to other parties. As a practical matter, that made virtually all use of online banking high risk. The new guidance provides that financial institutions should identify customers engaged in high risk transactions, which it now describes as transactions that present higher risk of financial loss or potential breach of information for which enhanced authentication controls are warranted. Factors in identifying high-risk transactions include the dollar amount and volume of transactions, the sensitivity and amount of information accessed, the irrevocability of the

Christopher Dodson

Member

cdodson@cozen.com
Phone: (215) 665-2174
Fax: (215) 372-2408

Andrew Baer

Chair, Technology, Privacy & Data Security

abaer@cozen.com
Phone: (215) 665-2185
Fax: (215) 372-2400

Related Practice Areas

- Technology, Privacy & Data Security

transaction, and the likelihood and impact of fraud. The 2021 guidance also introduces the concept of high risk users who might warrant additional controls. In identifying high risk users, financial institutions are expected to consider a user's access to critical systems and data, privileged users such as security administrators, remote access to systems, and users in key positions such as senior management.

Topics addressed by the 2021 guidance include:

- conducting a risk assessment for access and authentication to digital banking and information systems;
- identifying all users and customers for whom authentication and access controls are required;
- identifying customers involved in high risk transactions that warrant enhanced authentication controls, such as multifactor authentication;
- identifying high risk users that warrant enhanced authentication controls, such as multifactor authentication;
- periodically evaluating the effectiveness of authentication controls;
- implementing layered security to protect against unauthorized access;
- logging, monitoring, and reporting of activities to identify and track unauthorized access;
- identifying and mitigating risks from email systems, Internet access (such as risks from unrestricted or unmonitored Internet use on financial institution computers), customer call centers, and IT help desks;
- identifying and mitigating risks from access by a customer-permissioned entity (i.e., a third party given permission by a customer to access electronic account information) access to a financial institution's information systems;
- maintaining awareness and education programs on authentication risks for users and customers; and
- verifying the identity of users and customers.

The guidance also includes a list of specific authentication and access management controls that financial institutions should consider employing, such as device-based public key authentication, one-time passwords, and rate limits on log-in attempts. However, the FFIEC warns that the effectiveness of each control can vary over time as the threat landscape evolves. So, the controls employed should be re-evaluated periodically as the financial institution's ongoing assessments.

The application of guidance will vary based on each financial institution's operational complexity, technological capabilities, risk assessments, and risk tolerances. Financial services clients should begin to evaluate whether their current authentication frameworks are consistent with the FFIEC's new guidance.