PUBLICATION

FFIEC Updates Its Guidance on Authentication and Access Controls: Key Takeaways Financial Institutions Should Implement Now

Authors: Aldo M. Leiva, Matthew George White, Alexander Frank Koskey, III
August 24, 2021

On August 11, 2021, the Federal Financial Institutions Examination Council (FFIEC), the multi-agency authority responsible for issuing uniform principles and standards for supervision of financial institutions, published new guidance on "Authentication and Access to Financial Institution Services and Systems" (the Guidance). This Guidance is intended to address the current cybersecurity threat environment and replaces previous FFIEC guidance published in 2005 and 2011. Areas addressed include risk management practices relating to oversight of identification, authentication, and access solutions for customers, employees, and third parties that access digital banking services and financial institution information systems. Below are key elements of the Guidance, and a list of action steps financial institutions can implement to ensure the effectiveness of their authentication programs in light of this new Guidance.

Key highlights of the Guidance include:

1. Conducting risk assessments for access and authentication to digital banking and information systems;

2. Identification of all users and customers for which access and authentication controls are required, including those who may warrant enhanced authentication controls, such as multi-factor authentication;

3. Periodic evaluation of access and authentication controls;

4. Implementation of layered security to prevent unauthorized access;

5. Monitoring, logging, and reporting of activities to identify and trace unauthorized access;

6. Identification of risks from email systems, Internet access, customer call centers, and internal IT help desks, and implementing mitigating controls to address such risks;

7. Identification of risks from customer-permissioned entities accessing information systems, and implementing mitigating controls regarding same;

8. Maintaining awareness of and education on authentication risks for users and customers;

9. Verification of the identity of users and customers.

Financial institutions considering updating their practices in light of this new Guidance may consider the following steps:

10. Reviewing existing risk management policies and procedures to ensure proper inventories of devices, systems, software, digital banking services, users, and customers. Customers involved in high-risk financial transactions and users involved in high-risk activities may be assessed for additional or enhanced authentication controls.

11. Identifying threats with reasonable probability of impacting systems, data, or user/customer accounts, as well as reviewing actual or attempted incidents of security breaches, identity theft, or fraud.

12. Assessing adoption and implementation of layered security measures, such as multi-factor authentication, user time-out, network segmentation, monitoring, and transaction amount limits.

13. Reviewing monitoring, logging, and reporting processes and controls.

14. With regard to email systems and internet use, assessing implementation of secure configurations, multi-factor authentication, remote access controls, education and training of users, and software patches; reviewing implementation of software vendor and service provider controls for outsourced services; blocking browser pop-ups and redirects; and limiting running of scripting languages.

15. Ensuring training of customer call center staff and IT help desk representatives to avoid social engineering techniques in resetting passwords or providing any other credentials.

16. Updating customer awareness programs to guard against the latest phishing, social engineering, or other fraudulent activity, including confirmation of legitimacy of communications issued by the financial institution.

17. Reviewing customer identity verification measures and considering implementation of methods focused on detecting fraudulent activities, such as impersonation, and avoiding dependence on knowledge-based questions to verify identity.

Potential Legal Issues

When considering the above measures, financial institutions should also consult with legal counsel to assess the potential legal implications associated with implementing changes to access and authentication procedures. Some of these issues may include:

18. Directing an updated risk assessment, with third party vendors, of the impact of new measures on the financial institution's risk profile;

19. Updating the financial institution's information security plan and/or incident response plan as required, including revising and updating table-top simulations and other plan testing measures;

20. Notifying relevant insurance carriers as necessary;

21. Reviewing third-party or vendor contracts to assess the impact of the adoption of new measures on performance, notification, or other contractual obligations;

22. Documenting and retaining records related to training, customer awareness, and other risk-communication materials;

23. Communicating with customers regarding new authentication requirements; and

24. Ensuring consistency of description of security risks to customers in customer awareness programs to avoid compliance risks;

If you have any questions regarding these potential legal issues, adoption of measures to comply with the Guidance, or any other aspect of your cybersecurity and data protection program, please contact the authors Aldo M. Leiva, Matthew G. White, CIPP/US, CIPP/E, CIPM, PCIP or Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity Team.