FFIEC Issues New Cybersecurity and Data Privacy Guidelines for Mobile Banking

CONSUMER FINANCE | CYBERSECURITY AND PRIVACY | JUNE 30, 2016

Steven Blickensderfer

Mobile banking is a convenient and powerful tool that provides customers with a bevy of cutting-edge services, including mobile check deposits, on-the-go bill pay, and peer-to-peer payments. For financial institutions, this technology has the potential to increase customer satisfaction and decrease costs.

Unfortunately, mobile banking has been involved in many incidents of fraud and security breaches. This is partly because mobile banking requires the coordination of several entities unrelated to the financial institution, such as app developers, device manufacturers, telecommunication companies, and other third-party service providers. Poor risk management and inadequate security measures in the apps and services themselves are also to blame.

To address these growing security concerns, the Federal Financial Institutions Examination Council (FFIEC) recently issued a new appendix to the Retail Payment Systems portion of its Information Technology Handbook, called "Appendix E: Mobile Financial Services." In it, the FFIEC sets forth numerous guidelines to help examiners evaluate the risk management and mitigation processes of financial institutions and third-party service providers. Among them, the FFIEC recommends financial institutions:

- develop a layered approach to mitigate operational risks and prevent unauthorized access to sensitive data through use of multi-factor and biometric authentication;
- develop apps that do not retain sensitive customer information on the device, such as IDs and passwords, and "rigorously" test them for vulnerabilities annually;
- develop well-constructed third-party contracts with legal counsel to cover the types of data collected and circumstances related to data sharing; and
- reassess mobile service offerings and monitor for any legal and regulatory changes that may apply to mobile banking on an ongoing basis.

The FFIEC is not the only regulatory body calling for tighter security in this space. In November 2015, the New York State Department of Financial Services announced plans to institute new cybersecurity regulations for the firms it oversees, including use of multi-factor authentication. Those regulations are still forthcoming.