Financial Institution Compliance Update

August 2, 2016

This communication is designed to provide you with quick snapshots and timely perspectives on recent regulatory developments.

Guidance for Financial Institutions using Mobile Financial Services (MFS) for Payment Processing Activities

Background

On April 29, 2016 the FFIEC published Appendix E, **Mobile Financial Services** (MFS), to its Retail Payment Systems IT Booklet (http://ithandbook.ffiec.gov/4191). Appendix E is aimed at providing guidance for financial services institutions using MFS as part of their payment processing activities. The Appendix was created to address comments on the lack of technical detail and specific focus on MFS in existing FFIEC guidelines. Appendix E focuses on identifying and managing risks associated with MFS.

Relevancy

MFS involves the use of a mobile device (i.e., laptop computer, smart phone, tablet) to conduct banking transactions and to initiate retail payments. Customers' mobile transactions often emulate those initiated on traditional desktop computers. MFS provide more convenient transaction execution capabilities, such as the initiation or acceptance of mobile payments. As MFS includes the use of devices not under the institution's direct control for processing retail payments, the risk to the institution's payment processing environment is increased.

MFS poses elevated customer risks related to device security, authentication, data security, application security, data transmission security, compliance, and third-party management. Customers are often less likely to activate security controls, virus protection, or personal firewall functionality on their mobile devices, and MFS often involve the use of third-party service providers. The underlying MFS technology that creates the elevated risk is often not understood by Management.

Appendix E emphasizes an enterprise-wide risk management approach for institutions to effectively manage and mitigate strategic and operational risks associated with MFS. The Appendix begins with a section explaining MFS technologies and protocols. Subsequent sections summarize risk identification and measurement specific to MFS, methods of risk mitigation, and methods which can be used for monitoring and reporting on MFS risk.

The final section of the Appendix is a generic, high-level work program containing steps for assessing the adequacy of MFS risk mitigation. Although the work program is geared towards financial institutions, any business using MFS would benefit from following the procedures outlined in the program. An important feature of the work program is its emphasis on risk management processes that management should have in place, rather than merely checking for the existence of controls.

Recommendations

With the growing use of MFS, Management must identify the risks associated with the types of MFS being offered as part of the institution's strategic plan. In addition, Management must incorporate the identification of risks associated with mobile devices, products, services, and technologies into the financial institution's existing risk management process.

1. Identification of risks specific to MFS should be incorporated into the institution's risk management process.

    - Management should identify the risks associated with the decision to offer MFS and determine what types of MFS best fit with the strategic vision, goals, and risk appetite of the institution including:

        - **Technology Risk:** Management should identify unique technological risks associated with specific mobile devices. This will require an understanding of the functions and risks associated with MFS technologies such as Short Message Service (SMS), mobile-enabled Web sites and browsers, mobile applications, and wireless payment applications.

        - **Operational Risk:** Management should identify the risks involved with transaction initiation, authentication and authorization. When using MFS, basic device access controls such as personal identification numbers (PIN) may not be adequate to protect data stored on a mobile device because the controls could be circumvented by someone with unrestricted physical access to the device. In addition, the use of SMS text messaging within MFS presents risk as SMS data is transmitted in unencrypted format.

        - **Compliance Risk:** Management should identify the relevant compliance risks as they determine which MFS to offer. Management should ensure all third-party agencies involved in MFS function in accordance with applicable compliance requirements. Compliance risk with MFS is elevated in part due to its reliance on third-party service providers for data storage, data transmission, and intermediate payment processing. Consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used to provide the products and services.

2. Once risks have been identified, measurement of the likelihood and impact of the risks should be quantified. The results should be prioritized to determine which controls may be appropriate for MFS provided by the institution.

    - Risks should be measured not only for financial impact, but also for their potential effect on operations, compliance, human resources, and the institution's reputation.

    - Risk measurement is not a static exercise. The process should be ongoing to account for changes in the institution's finances, business operations, and external forces.

3. Management should mitigate identified risks by implementing effective controls across the institution. Management should develop and implement policies and procedures specific to MFS to comply with applicable laws and regulations. Appropriate internal controls for security and confidentiality of the MFS transactions should be put in place.

4. A robust monitoring and reporting process should be in place to enable Management to assess adherence to MFS guidelines, identify potential control deviations, and assess the effectiveness of risk mitigation processes. Monitoring requires establishment of limits on the level of acceptable risk exposure that management and the board are willing to assume.

    - Management should identify specific objectives and performance criteria, including quantitative benchmarks, for evaluating success of MFS.

- The monitoring process should include periodically comparing actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- Reporting should be tailored for the needs of various levels of management.

How Experis can help

Experis Finance offers industry experience in all aspects of Mobile Financial Services, including:

- Assessing the adequacy of your organization's MFS control environment
- Developing MFS programs to address unique risks
- Assisting in the development and/or enhancement of monitoring programs to detect misuse of the MFS environment
- Developing and maintaining first, second, and third line control and transaction testing

Our IT Risk Advisory Services practice can evaluate your current Mobile Financial Services program in relation to your organization, provide comprehensive recommendations for improvement and help address those recommendations.

Our team of professionals is experienced in working with clients to address these issues in order to help them avoid costly fines and penalties. If you have any questions about or concerns around your implementation of these steps, contact an Experis representative at financialservicesindustry@experis.com or visit our website Experis Finance.