Appendix E: Mobile Financial Services

AppE.1 Introduction

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices.[1] The mobile channel[2] provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ. As with other technology-related risks, management should identify, measure, mitigate, and monitor the risks involved and be familiar with technologies that enable MFS.

AppE.1.a Purpose and Scope

This appendix focuses on risks associated with MFS and emphasizes an enterprise-wide risk management approach to the effective management and mitigation of those risks. This appendix also discusses the technologies used in the mobile channel and may be helpful to the board and management for the integration of MFS into the institution's risk management program. The risks and controls addressed in this appendix, however, are not exhaustive. Additionally, this appendix contains a set of work program objectives to help the examiner determine the inherent risk and adequacy of controls at an institution or third party providing MFS.

AppE.1.b Background

MFS involve the use of a mobile device to conduct banking transactions and to initiate retail payments. Customers' mobile transactions often emulate those initiated on traditional desktop computers; however, MFS can provide more convenient transaction execution capabilities, such as the initiation or acceptance of mobile payments. MFS can pose elevated 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. This appendix addresses the following:

- MFS technologies.
- Risk identification.
- Risk measurement.
- Risk mitigation.
- Monitoring and reporting.

[1] A mobile device is a portable computing and communications device with information-storage capability.

[2] The mobile channel refers to providing banking and other financial services through mobile devices.

AppE.2 Mobile Financial Services Technologies

Financial institutions implement and offer MFS through technologies such as the following:

- Short message service (SMS)/text messaging.
- Mobile-enabled Web sites and browsers.
- Mobile applications.
- Wireless payment technologies.

AppE.2.a Short Message Service

SMS is a text messaging service component of phone, Web, or mobile communication systems. SMS uses standardized communications protocols to allow devices to exchange short text messages. Messages are typically limited to 160 characters and communicate either between mobile devices or between businesses and mobile devices (e.g., financial institutions requesting customer verification of transactions). Within the context of MFS, a customer uses SMS to provide financial transaction instructions to their financial institution. Financial institutions use SMS to provide information to customers, including account alerts or to communicate one-time passwords for Web site authentication.

AppE.2.b Mobile-Enabled Web Sites

A mobile device's browser allows customers to access a financial institution's Web site. Many financial institutions provide mobile-enabled Web sites, in addition to their regular Web site, which may improve the customer experience. The mobile-enabled Web site is designed to detect the type of device the customer is using (e.g., mobile device or desktop computer) and displays Web pages in the best format for that device.

AppE.2.c Mobile Applications

Mobile applications are downloadable software applications developed specifically for use on mobile devices. Mobile financial applications are developed by or for financial institutions to allow customers to perform account inquiries, retrieve information, or initiate financial transactions. This technology leverages features and functions unique to each type of mobile device and often provides a more user-friendly interface than is possible or available with either SMS or Web-based mobile banking.

AppE.2.d Wireless Payment Technologies

Customers may use mobile technologies to initiate wireless payments at point-of-sale (POS) terminals, make person-to-person (P2P) payments, or make other types of wireless payments, such as parking meter and mass transit access payments. Mobile wallets[3] allow customers to make wireless payments with a virtual payment card, as opposed to a physical card. The

[3] A mobile wallet is a front-end application that stores payment card information on the mobile device and allows payments to be made using a mobile device. The mobile wallet utilizes traditional retail payment channels such as ACH, EFT, and debit/credit card networks to process the payments.

exchange of payment credentials and authorization between the mobile device and the payment recipient can use different core technologies. Technologies that provide the ability to make wireless payments include the following:

- **Near field communication (NFC).** Wireless protocol that allows for exchange of payment credentials stored on the mobile device and other data at close range. For example, NFC is used to facilitate mobile payment systems developed by mobile phone manufacturers in conjunction with issuing financial institutions.
- **Image-based.** Coded images similar to bar codes used to initiate payments. Credentials may be encoded within an image or stored in the cloud. For example, specific retailers use quick response (QR) codes[4] to identify customers in a closed-loop mobile payment[5] system.
- **Carrier-based.** Payments billed directly to a customer's mobile carrier account. Merchants are paid directly by the mobile carrier, bypassing traditional payment networks. For example, a carrier-based payment may occur when mobile users donate money to charity through SMS messages.
- **Mobile P2P.** Payments initiated on a mobile device using the recipient's mobile phone number, e-mail address, or other identifier. Payment is through established retail payment technologies. For example, customers may download a P2P mobile application from their financial institution that allows them to send money to other users enrolled in the institution's system.

Although these technologies help facilitate financial institution-centric mobile payments, established retail payments channels (automated clearing house (ACH), credit/debit networks, electronic funds transfer (EFT), and intra-account transfers) remain the principal methods by which mobile payments are funded[6] and settled in the U.S. marketplace. With traditional retail payments channels serving as the backbone of mobile payments, users typically are required to provide verifiable financial institution account information or a credit, debit, or prepaid card to establish and fund a mobile payments service. The traditional retail payments channels allow financial institution mobile payments providers to leverage existing banking relationships to verify identities, satisfy federal anti-money laundering requirements, and fund accounts.

AppE.3 Risk Identification

Management should identify the risks associated with the types of MFS being offered as part of the institution's strategic plan. Management should incorporate the identification of risks associated with mobile devices, products, services, and technologies into the financial institution's existing risk management process. The complexity and depth of the MFS risk

[4] A QR code is a type of two-dimensional bar code or machine-readable optical label that contains information about the item to which it is attached.

[5] Closed-loop payments allow consumers to pre-load funds into a spending account that is linked to the payment device that can be used for purchases only at a specific company. Open-loop payments allow consumers to tie a mobile wallet to a personal account (e.g., credit card), do not require a prepaid amount, and spending is not limited to one company.

[6] Funding refers to adding a positive balance that customers use to make purchases.

identification varies depending on the functionality provided through the mobile channel and the type of data in transit and at rest.

The identification process should include risks at the institution and those associated with the use of mobile devices where the customer implements and manages the security settings. In providing customers with avenues for performing banking activities through mobile devices, an institution may transfer to the customer the ability to implement security settings. This transfer increases dependence on the customer to manage the controls over sensitive financial data. Additionally, there are numerous types of mobile devices that present different risks, and management should identify unique risks associated with specific devices. Before implementing mobile products and services, management should identify the associated risks, particularly in the areas of strategic, operational, compliance, and reputation risks.

AppE.3.a Strategic Risk

When financial institution management fails to incorporate its decisions regarding MFS into its strategic planning, the institution's level of strategic risk may increase. 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.

AppE.3.b Operational Risk

MFS introduce unique operational risks. Management should identify the risks involved with transaction initiation, authentication and authorization, and the MFS technology itself. Some of the operational risks are associated with the mobile device and how the device communicates with the POS or other similar terminal.[7] Additionally, the varying access points[8] provide challenges with authentication and security.

MFS provide the opportunity to leverage tools and techniques not available in traditional banking payment products. The prevalence of mobile devices, common operating systems, and downloadable applications make these devices a target for malware and viruses. Without implementing additional controls, basic device access controls such as personal identification numbers (PIN) may not be adequate to protect data that is stored on a mobile device because these controls could be circumvented by someone who has unrestricted physical access to the device. Additionally, a fraudster can compromise mobile application-based financial services by developing rogue, corrupted, or malicious applications (or adding rogue code to applications) that a customer downloads to his or her mobile device. Therefore, management should consider the implications of operational risks when evaluating and implementing such technologies.

[7] Traditional payment risks associated with the underlying payment transaction are covered by existing risk management guidance contained in earlier sections of this booklet.

[8] Access points include a user's home network, cellular network, NFC, Bluetooth, or public Wi-Fi connections, such as those provided by a municipality or business.

AppE.3.b(i) SMS Technology Risk

SMS technology presents a number of security-related risks. SMS messages typically are transmitted unencrypted over widely used telecommunications networks. The messages are also vulnerable to spoofing,[9] which allows an unauthorized user to send an SMS message pretending to be from a different mobile number to mislead a customer into providing sensitive information to the unauthorized user. Similarly, fraudulent SMS messages may mislead customers into revealing financial institution account information or information used to access financial institution systems.

AppE.3.b(ii) Mobile-Enabled Web Site Risk

Mobile-enabled Web sites rely on existing Internet security protocols, which make the sites subject to many of the same vulnerabilities[10] that can compromise computer-based banking. Additionally, mobile devices can be limited by their hardware and operating systems, which can result in a reduced level of security. Mobile Web browsers are common starting points for malicious attacks, and malicious messages can come from many other sources.[11] Whereas desktop browsers have anti-phishing[12] and anti-cross-site scripting (anti-XSS) capabilities[13] to filter out the malicious code from Web sites, mobile-enabled browsers do not always have such features. The lack of anti-phishing and anti-XSS modules can increase the possibility of loss of sensitive information when using a mobile device.

As is the case with any Web-based application, attacks involving unvalidated "redirects and forwards"[14] can be used to maliciously craft a URL[15] to bypass the application's access control check and then provide the attacker access to privileged functions that normally would not be accessible to them. The attacks also can lead to malware download and installation. By modifying a URL and redirecting the browser to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.

[9] SMS spoofing is the manipulation of address information to impersonate a user.

[10] Vulnerabilities include malware attacks, eavesdropping, and spoofing.

[11] Besides e-mail and instant messages, sources can also include SMS, social messengers, hypertext markup language (HTML) links, and QR codes.

[12] Anti-phishing software are programs, either integrated with or built in to the Web browser, that display the real domain name of the site that a user is visiting to help prevent fraudulent sites from posing as legitimate sites.

[13] Anti-XSS functionality is a defense mechanism to XSS, which is a vulnerability found in Web applications that enables attackers to inject client-side script into Web pages prompting a Web page to display unvalidated user input. Attackers may use this vulnerability to bypass access controls.

[14] Unvalidated Web site redirects are possible when a Web application accepts untrusted input that could cause the application to redirect the request to a malicious URL. A user may be redirected and not realize it.

[15] URL is an acronym for uniform resource locator and is a reference (an address) to a resource on the Internet.

Users often find it difficult to recognize a phishing message or a forged Web site, or determine whether a site is safe. Additionally, mobile browsers displayed on small screens may not effectively display the same visual security cues more easily seen on full-scale browsers on large screens.

AppE.3.b(iii) Mobile Application Risk

Applications can be downloaded onto mobile devices from a number of application stores. Although device manufacturer-authorized application stores perform due diligence, applications may still contain vulnerabilities that cause risks to the user and the financial institution. On some mobile devices, it is possible to download an application from application stores not authorized by the manufacturer, which poses a greater risk of users being exposed to malicious code because the applications may not be adequately reviewed by the store. Distribution of malware through applications is a material risk to the institution and its customers because of malware's ability to compromise sensitive data and monitor communications.

Another risk to the institution and its customers occurs with the end user's ability to access root user[16] privileges in the operating system of the device. The process to gain access is known as "rooting." Another method of removing the manufacturer's device controls or core operating system controls is "jailbreaking." Jailbreaking provides the user with additional access to and control over the device's operating and file systems, including the ability to circumvent security controls. For certain mobile devices, rooting and jailbreaking allow the user to download applications from untrusted sources, which may introduce malware onto the device.

Many applications store usernames, passwords, and e-mail addresses in clear text. Because users often have the same usernames and passwords across systems, it is possible to use the information obtained from a poorly designed mobile application to compromise user accounts on other systems. Mobile applications collect personal information (e.g., name, account number, and other personal details) and track user activity (e.g., purchases and location). These data are valuable to attackers and can result in compromised user privacy. Without properly securing the mobile application, unauthorized users can gain access to the back-end databases containing confidential information.

The mobile ecosystem is the collection of carriers, networks, platforms, operating systems, developers, and application stores that enable mobile devices to function and interact with other devices. Vulnerabilities may exist in any area of this decentralized mobile ecosystem and, therefore, result in a multi-entity patch management process among mobile device operating system developers, device manufacturers, wireless carriers, and other application developers. As a result of the decentralized ecosystem of some devices, a known vulnerability may remain unremediated while the various parties review, update, and ensure compatibility with their applications and the security mitigation. Additionally, integrating MFS application functionality with other applications and services on the customer's device may introduce vulnerabilities because MFS applications are not built in or native to the device.

[16] The root user is the conventional name of the user who has all rights or permissions to all files and programs. Having such rights or permissions allow the root user to do many things an ordinary user cannot.

AppE.3.b(iv) Mobile Payments Risk

The portability of mobile devices can lead to the devices being misplaced or stolen, which may allow unauthorized access to the mobile wallet or user credentials. Such access can result in unauthorized payments and funds transfers and fraudulent purchases.

Because mobile payments at the POS may use NFC, communications between the device and the POS terminal can be intercepted, while the device is in the user's possession. Even if these communications are encrypted, which they are not by default, there remains a potential for unauthorized access to transaction information, which could be used to perpetrate financial fraud.

Vulnerabilities create the potential to take advantage of weak security controls in the payment provisioning or enrollment functions of the NFC payment system process to commit fraud. Malicious actors using stolen identity information (e.g., from credit reports, tax records, health care records, and employee records) may establish fake accounts on NFC-enabled mobile devices to make unauthorized transactions.[17]

AppE.3.c Compliance Risk

Financial institution management should identify the compliance risks as it determines which MFS to offer and continue to monitor these risks as the technology for MFS evolves. 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.

One of the challenges in providing MFS is that a significant portion of the innovation in the industry is driven by entities outside of the traditional financial services sector. These entities may be unfamiliar with regulatory requirements and supervisory expectations that apply to regulated financial institutions and their service providers. Management should understand how the institution's risk profile changes when it uses any third party, but particularly a third-party service provider that is unfamiliar with the regulation and supervision of the financial services sector, to design applications.

AppE.3.d Reputation Risk

Management should identify and consider how providing MFS may create reputation risk. Reputation risk is particularly relevant in the context of privacy and data security, as public scrutiny of the treatment of customer information continues to grow. The mobile channel, with many of its activities trending toward personalization[18] and transmission of data, poses a risk of disclosure of personal information. Additionally, services provided by a third party that are not implemented appropriately or securely may expose the financial institution to reputation risk if interruptions in service occur or sensitive customer information is compromised.

[17] Refer to U.S. Secret Service and PCI Security Standards Council, "Joint Advisory Bulletin: Mobile Payment System Vulnerability," September 2015.

[18] Personalization is providing a tailored user experience based on user preferences through MFS.

AppE.4 Risk Measurement

The identification of risks should be followed by a measurement of the level and types of risks involved in offering MFS. Management should measure potential risks across all applicable risk categories. This assessment may help management determine the likelihood and impact of the risks affecting the institution. The results should be prioritized to determine which controls may be appropriate for the services provided by the institution. This process should be ongoing and updated whenever management implements a change to the strategy or MFS.

AppE.5 Risk Mitigation

Effective enterprise-wide risk management helps management determine whether controls are effective and goals are compatible with the financial institution's risk appetite and strategic plan. When offering MFS, management should mitigate identified risks by implementing effective controls across the institution. As is the case with any new product offering, management should develop and implement policies and procedures to comply with applicable laws and regulations and require appropriate internal controls for security and confidentiality of the MFS transactions. As part of the institution's audit of retail payments systems, audit coverage should include MFS.

Unlike many financial services that allow institutions to control much of the interaction, MFS typically require the coordinated and secure exchange of information among several unrelated entities. Depending on the type of MFS offered, institutions may find that the effective management of risks involves interaction with application developers, mobile network operators, device manufacturers, specialized security firms, and other nonfinancial third-party service providers. Additionally, financial institution management should provide security awareness materials to the institution's customers, which may include prudent security practices for the device (e.g., use of mobile anti-malware, PIN protection) so that customers understand their roles in securing the device and the need for such security.

AppE.5.a Strategic Risk Mitigation

Financial institution management should incorporate decisions on providing MFS into its strategic planning process. Various elements should be part of any mobile strategy, including the products and services to be offered, types of transactions allowed, limits over transaction amounts, mobile architecture design, supported mobile devices, customer needs, and use of third parties.

AppE.5.b Operational Risk Mitigation

Financial institution management should develop a layered approach to mitigate operational risks from MFS. This may include implementing security techniques at the server and database level; using transaction monitoring and geolocation techniques to identify anomalous MFS transactions; implementing and refining fraud prevention, detection, and response programs that facilitate rapid notification of potentially fraudulent transactions; applying additional controls (e.g., stronger authentication, encryption) to prevent unauthorized access to sensitive customer

information stored on the device; and educating customers and employees to identify social engineering attempts that could lead to fraud.

The following are general operational controls that an institution should consider when implementing MFS.

- **Enrollment.** Financial institution management should have appropriate controls and communication of policy and procedures to verify a customer's identity when enrolling customers in mobile payment systems used at the point of sale (e.g., allowing a customer with a physical payment card the ability to enroll that card into the customer's mobile wallet).
- **Authentication and authorization.** A financial institution should have a process for authenticating users of MFS to protect customers against fraudulent transactions or malicious activities. Depending on the technology used and associated level of risk, financial institutions may consider biometric (e.g., voice, fingerprint, facial recognition) or out-of-band[19] authentication processes. The financial institution should not use mobile payment applications that rely on less secure (e.g., single factor) methods of authentication.[20]
- **Application development and distribution.** The application development life cycle should include a thorough design and architecture review using threat-modeling[21] techniques to reduce potential risks and meet the financial institution's security objectives. Additionally, application developers should develop applications using secure coding techniques,[22] and applications should be rigorously tested for vulnerabilities (e.g., detailed code analysis and white-hat hacking[23]) at least annually. Institutions should distribute applications and updates securely and in a timely fashion. Management should consider designing anti-malware capabilities into mobile applications. Applications should not retain sensitive customer information on the device, such as user IDs and passwords, and the application should securely wipe any sensitive customer information from memory when the customer exits the

[19] Out-of-band refers to activity outside of the primary means of interfacing with the customer. For example, if a user is performing activity online, he or she may be authenticated through a one-time password sent via text message.

[20] Resources that provide detailed information about authentication for financial institutions include: FFIEC Authentication Guidance (http://www.ffiec.gov/pdf/authentication_guidance.pdf), Frequently Asked Questions (https://www.ffiec.gov/pdf/authentication_faq.pdf), and Authentication Supplement (https://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf).

[21] Threat modeling is a structured approach that enables an institution to aggregate and quantify potential threats. In the context of application development, threat modeling can be used to capture, organize, and analyze all of the threat information of an application and its environment that affects application security. It is used to enable informed decision-making about application security and helps to produce and rank a list of security improvements.

[22] Secure coding is the process of developing code (e.g., Web application) with security built in during the development process using technical controls to mitigate the occurrence of software vulnerabilities.

[23] White-hat hacking, also called ethical hacking, refers to the specialization of penetration testing and other testing methodologies to review the security of an institution's information systems by determining flaws and vulnerabilities.

application. If a third party developed the application, the third-party developer should incorporate these control requirements into its development process.

- **Application security.** Management should ensure that the institution's MFS contain log-on credentials in addition to those used to access the device. Management should employ multi-factor authentication or layered security controls depending on the types and volumes of transactions. The system should require re-authentication whenever the device or MFS is unused for a designated period and each time the user launches the application.
- **Contracts.** The institution should use well-constructed contracts, developed with legal counsel, to mitigate its risks from third parties. Contracts should be appropriate for the institution's specific mobile strategy and should clearly identify each party's roles and responsibilities. Financial institution management may need to establish contracts with the institution's customers and third parties that cover types of data collected and circumstances related to data sharing.
- **Customer awareness.** Financial institution management should make reasonable efforts to educate customers about the need to maintain the physical and logical security[24] of mobile devices and suggest that users regularly install operating system and firmware updates. Management should make clear that customers should download applications only from reputable sources, and the institution's Web site should have a link to the source of any institution-approved applications. Institutions should have customer security awareness materials available to help customers understand the risks involved in using MFS, including the use of unsecured "public" wireless networks. Financial institutions should suggest that customers consider running anti-malware software on their mobile devices, if possible.
- **Logging and monitoring.** Management should have logging and monitoring capabilities on all MFS to track customer activity and security changes and identify anomalous behavior and transactions.

AppE.5.b(i) SMS Technology Risk Mitigation

Financial institution management should employ compensating controls (e.g., redacting customer account numbers when sent via SMS) to mitigate the inability to encrypt SMS messages. Additionally, management should limit the access or functionality available to the customer through SMS banking. When the transaction risk is more significant, management should consider other risk mitigation methods, including pre-registration and the use of security tokens. PINs also could be employed, but are often easier to break and harder to remember. To strengthen the security of PIN usage, management can implement specific requirements (e.g., requiring them to be regularly changed). An institution should update its customer awareness materials to include information on avoiding phishing messages by SMS.

AppE.5.b(ii) Mobile-Enabled Web Site Risk Mitigation

Financial institution management should consider several controls to mitigate risks associated with mobile-enabled Web sites, including the following:

[24] Prudent security practices may include information on the use of the device's password function, general safeguards, and any additional logical security controls (e.g., available security applications).

- Provide specific training and security awareness materials for users and customers accessing the institution's sites to teach them how to identify compromised sites.
- Require Web site developers to follow a secure development life cycle to increase the security of the Web sites designed for the financial institution.
- Require developers to build a secure Web site especially for mobile devices and encourage them to follow the guidelines provided from the Open Web Application Security Project (OWASP)[25] Top 10 for Web application and OWASP Top 10 for mobile.
- Make available a baseline set of controls, and educate customers on the use of those controls to protect their device and information (e.g., device passwords with complexity, application passwords, and an auto-wipe feature after excessive password failures).
- Determine whether mobile browsers have available safeguards implemented, such as anti-XSS modules or additional monitoring of browsers for those that are no longer supported, and deny access to devices with mobile browsers not meeting minimum standards.
- Determine whether mobile-enabled Web sites are designed with the following mitigating controls to help minimize the potential for exploitation of "redirect and forward" vulnerabilities:
  - Avoid using redirects and forwards.
  - Explicitly hard code the URL to prevent manipulation by an attacker.
  - Apply additional validation or control checks to verify the user trying to access the URL, validate the URL, check the appropriateness of the URL request, and prevent a malicious user from redirecting site users to a phishing, malicious, or nonaffiliated site.
  - Create a whitelist[26] of trusted URLs.
  - Force all redirects to go through a page that notifies a user that he or she is leaving the page and require user confirmation.
  - Perform frequent vulnerability scans.

AppE.5.b(iii) Mobile Application Risk Mitigation

Management should consider the use of a variety of security mechanisms for mobile applications and should evaluate, prioritize, and implement appropriate mitigating controls, including the following:

- Employing tools, such as policy enforcement and device fingerprinting, to determine whether a customer's mobile device will be allowed to access the institution's MFS by validating device characteristics (e.g., level of security controls, operating system type, operating system version, whether the mobile device is rooted or jailbroken, and patch status).
- Providing security awareness training to end users to help them recognize legitimate applications and provide a list of reputable sites to download institution-approved applications.
- Performing security testing at all post-design phases of the system development life cycle for all applications. Establishing a process to deactivate older application versions that no longer

[25] OWASP is an online community dedicated to Web application security.

[26] A whitelist is a list of trusted entities. With respect to URL redirects, an institution can create a whitelist of allowable URLs.

meet minimum security requirements or prompt the end user to upgrade to an acceptable version.

- Providing basic customer education relative to security to mitigate the risks associated with rooted or jailbroken devices.
- Designing applications to ensure that critical information, such as passwords and credit card numbers, does not reside directly on a device. If critical information resides directly on a device, it should be stored securely (e.g., within an encrypted data section or within encrypted storage in the file system).
- Establishing processes when implementing mobile applications to collect only necessary information and appropriately secure that information and any related analytics reporting available within or external to the mobile application.
- Designing applications to mitigate the risk of unpatched devices or those that are no longer supported by the manufacturer.
- Securing back-end servers containing the MFS application and customer data to prevent unauthorized users from accessing data. If a third party manages the application and back-end server, validate that the third party implements appropriate security measures.
- Developing applications in a "sandbox,"[27] which creates a more secure area within the device from which to process transactions.
- Maintaining awareness of vulnerabilities through online forums, vendor sites, and U.S. Computer Emergency Readiness Team (US-CERT) or Financial Services-Information Sharing and Analysis Center (FS-ISAC) alerts. The vulnerabilities may affect unpatched and unsupported operating system versions. Take a risk-based approach when offering MFS to customers using unpatched and unsupported operating system versions and recommend to customers that they upgrade to more secure software, operating systems, and devices when appropriate.
- Periodically testing the functionality of MFS applications with other integrated mobile applications and services.

AppE.5.b(iv) Mobile Payments Risk Mitigation

Mitigating controls in mobile payments should include discussions between the financial institution and its mobile payments provider to identify and minimize potential risk factors. Financial institution management should work with mobile-payments platform developers to encourage the use of the following:

- Traffic filtering to help prevent or minimize denial-of-service attacks.[28]

[27] A sandbox is a restricted, controlled execution environment that prevents potentially malicious software, such as malicious mobile code, from accessing any system resources except those for which the software is authorized.

[28] The goal of a denial-of-service attack is to restrict the availability of services or systems. If the institution can effectively filter traffic to disallow unknown or potentially malicious traffic, this can support the institution's larger denial-of-service planning.

- Trusted platform modules.[29]
- Secure telecommunications protocols (e.g., secure sockets layer/transport layer security [SSL/TLS]).
- Tokenization[30] to limit the transmission of account information.
- Encryption to minimize the opportunity for the interception of traffic.
- Anti-malware software.
- Authentication controls of both the user and application.
- Encryption of personal information stored on the mobile device.

AppE.5.c Compliance Risk Mitigation

Institution management and system designers should consult with compliance staff to minimize compliance risks when developing and implementing MFS. Financial institution management should reassess its current mobile service offerings regularly and, in conjunction with appropriate compliance and legal staff, examine applicable laws and regulations, including those for consumer protection, to determine which may apply to their specific mobile financial service offerings. The compliance officer should take the following steps:

- Determine whether applicable disclosure requirements are fully accessible on the mobile device.
- Review the institution's existing compliance management system and ability to make appropriate modifications to policies and procedures to address the products, services, and operating features of the MFS technology.
- Monitor for any legal and regulatory changes that may be applicable to MFS on an ongoing basis.
- Train institution staff regarding compliance implications of MFS.

AppE.5.d Reputation Risk Mitigation

To protect its brand reputation, management should adopt appropriate and effective controls over customer information accessed, transmitted, or stored by the MFS to minimize or prevent disclosure of personal information and the potential for fraudulent transactions. Management should implement such controls whether it is providing the MFS directly or through a third party.

AppE.6 Monitoring and Reporting

Financial institution management should have appropriate performance monitoring systems for assessing whether the product or service is meeting operational expectations. Such systems should do the following:

[29] The trusted platform module is an international standard for a secure crypto processor that is a dedicated microprocessor designed to secure hardware by integrating cryptographic keys into devices.

[30] In the context of data security, tokenization is the process of substituting a sensitive data element with a surrogate value, referred to as a token.

- Include limits on the level of acceptable risk exposure that management and the board are willing to assume.
- Identify specific objectives and performance criteria, including quantitative benchmarks for evaluating success of the product or service.
- Periodically compare actual results with projections and qualitative benchmarks to detect and address adverse trends or concerns in a timely manner.
- Modify the business plan, when appropriate, based on the performance of the product or service. Such changes may include exiting the activity should actual results fail to achieve projections.

A variety of reports can facilitate management oversight of MFS activities. Management should structure the report content to meet the needs of the various levels of management. Reports should address point-in-time as well as trend activity for both individual customers and mobile channel activities to compare actual trends with the mobile strategy. Reports for new services should emphasize the volume of activity from the onset and report on changes in usage or volume over time. Management should develop reports to document the various demographic and industry sectors served and monitor changes in these areas to determine whether the MFS offered are meeting the institution's strategy or should be refined.

AppE.7 Mobile Financial Services Work Program

Objective 1: Management effectively responds to issues raised or problems related to MFS.

1. Review examination documents and financial institution reports for outstanding issues or problems related to MFS. Consider the following:

    a. Pre-examination planning memos.
    b. Prior regulatory reports of examination.
    c. Prior examination work papers.
    d. Internal and external audit reports, including SSAE 16[31] reports.
    e. Financial institution's overall risk assessment and strategic plan.

2. Review management's response to audit recommendations on MFS, if any, noted since the prior examination. Consider the following:

    a. Adequacy and timing of corrective action.
    b. Resolution of root causes rather than just specific audit deficiencies.
    c. Existence of any outstanding issues.
    d. Monitoring systems used to track the implementation of recommendations on an ongoing basis.

[31] Statement on Standards for Attestation Engagements (SSAE) No. 16 is a type of audit report of controls at a service organization.

Objective 2: Financial institution management incorporates (or plans to incorporate) its plan for implementing MFS into its strategic planning process.

1. Determine whether financial institution management has an MFS strategy to identify the types of MFS that management plans to offer.

2. Describe the MFS that the financial institution offers. Determine whether the institution offers or implements MFS through one or more of the following technologies:

    a. SMS.
    b. Mobile-enabled Web sites or browsers.
    c. Mobile applications.
    d. Technologies that enable mobile payments.

Objective 3: Financial institution management identifies the risks associated with offering MFS.

1. After the MFS strategy is complete, determine whether the institution developed an effective risk assessment process for the MFS offerings. Verify whether management incorporates the results of the risk assessment into a process to periodically review and update the strategy.

2. Review whether the risk identification process includes risks associated with MFS, particularly in the areas of strategic, operational, regulatory, and reputation risks.

3. With respect to strategic risk, determine whether management identified the risks associated with the decision to offer MFS and whether that is consistent with the strategic vision, goals, and risk appetite of the institution.

4. Determine whether management considered and identified operational risks associated with MFS, including risks involved with the following:

    a. Transaction initiation and completion.
    b. Authentication and authorization.
    c. Technology used for MFS.
    d. Mobile devices.
    e. Method of communication between the device and the terminal accepting payment.
    f. Authentication and security of access points.
    g. Fraud tools and techniques.
    h. Current and emerging threats to mobile applications, weaknesses in mobile application security, and prevalence of mobile devices, common operating systems, and downloadable applications.

5. Determine whether management also considered the implications of operational risks specific to technologies used to implement MFS. Specifically, review whether management appropriately identified the differing risks related to the following technologies:

a. **SMS:** Include the lack of security through unencrypted text messages; SMS spoofing; and fraudulent text messages (phishing).
b. **Mobile-enabled Web sites:** Include vulnerabilities with Internet banking (hardware, operating system, and security limitations); malicious messages through Web-based attack vectors; limitations on anti-phishing and anti-XSS capabilities; malicious attacks through unvalidated redirects and forwards; user constraints on recognizing phished or forged sites; and limitations on visual security cues.
c. **Mobile application:** Include application vulnerabilities (e.g., unpatched and outdated applications); malware; ability to jailbreak or root devices; use of unapproved application stores; weak storage controls over confidential information on devices; and inappropriate access to back-end databases.
d. **Mobile payments:** Include loss or theft of mobile devices leading to unauthorized payments, funds transfers, and credit card purchases; interception of NFC communications; and weak security controls in the payment provisioning process.

6. With respect to compliance risk, determine whether management identified the applicable risks related to MFS. Review whether management understands that the consumer laws, regulations, and supervisory guidance that apply to a given financial product or payment method generally apply regardless of the technology used. Additionally, determine whether management identified risks associated with the use of nontraditional third-party service providers often found in the innovation and development sphere of MFS.

7. With respect to reputation risk, determine whether management identified the following:

   a. Potential reputation risk that may arise from providing MFS, including issues related to privacy and data security.
   b. Risks associated with the decision to outsource the development and maintenance of mobile products and the effect of third parties on the institution's risk profile.

Objective 4: Financial institution management appropriately and effectively measures risks associated with MFS and determines the likelihood and impact of those risks.

1. Determine whether management effectively measures risks and determines the likelihood and impact of those risks.

2. Determine whether management effectively prioritizes measured risks.

3. Determine the effectiveness of the frequency of the measurement process.

Objective 5: Financial institution management effectively identifies and implements controls to mitigate identified and prioritized risks associated with the MFS offering.

1. Determine whether management incorporates mobile risks into the overall risk management process.

2. Determine whether management implements policies and procedures for the MFS offering.

3. Determine whether management puts in place appropriate internal controls to ensure security and confidentiality of MFS.

4. Determine whether management implements controls to mitigate all applicable categories of risks related to MFS, including strategic, operational, compliance, and reputation risk.

    a. **Strategic risk mitigation:** Review whether management incorporates its decisions to provide MFS into its strategic planning process.
    b. **Operational risk mitigation:** Review whether management controls include the following: risk management; transaction monitoring and geolocation tools; fraud prevention, detection, and response programs; additional controls (e.g., stronger authentication[32] and encryption); authentication and authorization processes (e.g., processes to enroll customers and devices in the mobile channel); application development and distribution controls (e.g., process for approving and submitting mobile application code to distribution partners); application security controls (including strategy to deactivate older application versions); contracts and agreements; customer awareness processes; and logging and monitoring processes. Specifically, review the controls that management has in place over the technologies employed for MFS, including the following:
        - SMS technology.
        - Mobile-enabled Web sites.
        - Mobile application.
        - Mobile payments.
    c. **Compliance risk mitigation:** Review whether management consults with compliance staff, reassessing current mobile service offerings regularly and examining for compliance with applicable laws and regulations.
    d. **Reputation risk mitigation:** Review whether management includes the use of controls to minimize or prevent disclosure of personal information and the potential for fraudulent transactions. Also, review management's mitigation of risks associated with the use of a third party, if applicable.

5. Determine whether management has appropriate and independent testing of controls for effectiveness.

Objective 6: Financial institution management maintains effective oversight of MFS activities. Management maintains appropriate reporting for various levels of management to support that oversight.

1. Review the monitoring process to determine whether the institution has appropriate performance monitoring systems to allow management to assess whether the product or service is meeting operational expectations. Determine whether the systems include the following features:

[32] A review should include the financial institution's consideration of expectations set forth in appropriate supervisory guidance (e.g., authentication guidance in footnote 20 of this appendix).

a. Limits on the level of acceptable risk exposure that management and the board are willing to assume.
b. Specific objectives and performance criteria to evaluate success of the product or service.
c. Ability to produce reports that periodically compare actual results with projections and qualitative benchmarks that provide trend information.
d. Ability to produce reports that provide data, which would trigger changes in the business plan, as appropriate.

2. Determine whether the institution's reporting process describes the following:

a. MFS activities.
b. Information to meet the needs of the various levels of management.
c. Trends, volumes, and changes in activity over time.
d. Statistics on demographics and locations served to evaluate whether the institution is meeting its strategy.

Objective 7: Discuss corrective action and communicate findings.

1. Review preliminary conclusions with the examiner-in-charge (EIC) regarding the following:

a. Violations of laws and regulations.
b. Significant issues warranting inclusion as matters requiring attention or recommendations in the report of examination.
c. Proposed URSIT[33] management component rating and the potential impact of the conclusion on composite or other component information technology ratings.
d. Potential impact of the conclusions on the institution's risk assessment.

2. Discuss findings with management and obtain proposed corrective action for significant deficiencies.

3. Document conclusions in a memorandum to the EIC that provides report-ready comments for all relevant sections of the report of examination and guidance to future examiners.

4. Organize work papers to ensure clear support for significant findings by examination objective.

[33] Uniform Rating System for Information Technology.