E IS FOR EXPOSURE

Appendix E and the Role of Vendor Management in Controlling Mobile Financial Services Risk

ncontracts
Risk Management Solutions

(888) 370-5552
info@ncontracts.com
www.ncontracts.com

EXECUTIVE SUMMARY: Financial institutions don't have complete control of the mobile channel. App developers, mobile network operators, device manufacturers, specialized security firms and other nonfinancial third-party service providers all play a role—making vendor risk management critical when providing mobile financial services. A review of the FFIEC's Appendix E: Mobile Financial Services demonstrates the importance of identifying, measuring, mitigating and monitoring risks presented by third-party providers, particularly in the areas of compliance risk, reputation risk and contracts.

Introduction

Few things today feel more personal than mobile devices. They hold intimate pieces of users' lives—photos, emails, texts, social media, music, payments and financial data. Yet as personal as smartphones, tablets and other devices feel, they are not that private. App developers, mobile network operators, device manufacturers, specialized security firms and others all play a role in making these machines run and work—and they all present security concerns.

It's troubling for users—and their financial institutions. 2015 marked the first time banks had more weekly mobile bankers (30 percent) than branch bankers (24 percent), according to Javelin Research.[1] As customers continue to seek out the convenience of mobile channels, it's become more and more critical for FIs to manage the risks of mobile financial services, particularly the role of third parties.

The Federal Financial Institutions Examination Council (FFIEC) drew attention to this issue in April when it revised the *Retail Payment Systems* booklet of the FFIEC Information *Technology Examination Handbook* (IT Handbook). The newly added *Appendix E: Mobile Financial Services* highlights the risks mobile financial services present to FIs as well as strategies for managing and mitigating those risks.

That includes:

- Risk identification
- Risk measurement
- Risk mitigation
- Monitoring and reporting

This isn't fully new territory. Regulators have ratcheted up attention to both cybersecurity and third-party vendor management over the past few years. Examples include the FFIEC's Cybersecurity Assessment Tool released in June 2015 (which frequently mentioned third-party connections, relationships and providers), Appendix J: Strengthening the Resilience of Outsourced Technology Service released in February 2015 and other guidance issued by individual agencies over the years.[2] These documents lay out a framework for effective third-party vendor risk management: identifying, measuring, monitoring and mitigating risk.

Appendix E builds on this framework to address some of the specific risks of the mobile environment, giving FIs direction on how to best manage this complex risk ecosystem—including objectives for measuring and assessing third-party provider risks and controls.

[1] Mobile Banking Outpaces Branch Banking for First Time in 2015. Javelin Research. January 2016. https://www.javelinstrategy.com/press-release/mobile-banking-outpaces-branch-banking-first-time-2015

[2] The most recent guidance since March 2016.
FRB: http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf
OCC: http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Deciding to offer mobile financial services is big step for any financial institution—not just because of the opportunities, but because of the risk.

Defining Mobile Financial Services

Mobile financial services go way beyond Internet banking. As defined by Appendix E, they include all "products and services that a financial institution provides to its customers through mobile devices." These technologies typically piggyback on existing networks including automated clearing house (ACH), credit/debit networks, electric funds transfer (ETF) and intra-account transfers.

They include:

- **SMS/Text messaging.** FIs can push information like account alerts to customers, and customers can send brief instructions to their FIs or confirm their identities.
- **Mobile-enabled websites.** When an FI notices a user on a mobile device, it can display a page specifically designed for that type of device in stead of the FIs traditional desktop page.
- **Mobile apps.** Users can download special applications allowing them to conduct banking transactions from their device. This can include checking balances, transferring funds and depositing checks.
- **Wireless payments.** These allow customers to conduct point-of-sale, person-to-person and other payments without a physical card. Examples include:
  - **Near field communications (NFC).** Enables contactless payments like Apple Pay by transferring payment information stored in a device over a short distance.
  - **Image-based.** Using coded images like QR codes to make payments, often from a pre-loaded card with a specific company. For example, Starbucks customers can display a QR code on their phone to pay. Other apps allow customers to pay by scanning a QR code on their bill.
  - **Carrier-based.** Payments—often made via text message—billed to the mobile carrier. This is popular for charitable donations where people are encouraged to text to a number to donate.
  - **Mobile P2P.** Payments initiated on mobile devices that use established retail payment technologies.

Identifying Third-Party Mobile Risk

Deciding to offer mobile financial services is big step for any financial institution—not just because of the opportunities, but because of the risk. Any FI that moves into this area must have a strategic plan for implementation that ties into the institution's overall enterprise risk management program, the appendix says. That includes identifying potential risks and having a plan for defending against them.

While vendor management can be complicated in any area, mobile financial services raises the stakes. Even customers introduce risk since they are often lax when it comes to "activate[ing] security controls, virus protection, or personal firewall functionality on their mobile devices," the appendix notes.

This makes managing third-party vendors all the more important. "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," notes Appendix E. Any one of these providers can be the source of a vulnerability and because the parties aren't centralized, problems aren't always immediately resolved since so many different groups need to work on it.

FDIC: https://www.fdic.gov/news/news/financial/2014/fil14013.html
NCUA: http://www.ncua.gov/resources/documents/ lcu2007-13enc.pdf
CFPB: http://files.consumerfinance.gov/f/201204_ cfpb_bulletin_service-providers.pdf

When it comes to oversight of third-party providers and MFS, Appendix E emphasizes two kinds: compliance risk and reputation risk.

Guidance tells us that risk comes in many forms, including compliance risk, reputation risk, operational risk, credit risk, strategic risk, transaction risk and cyber risk.[3] Appendix E goes into detail about operational risk and the many technical risks presented by different MFS technologies. When it comes to oversight of third-party providers and MFS, Appendix E emphasizes two kinds: compliance risk and reputation risk.[3]

Compliance Risk

It's a tired refrain by now, yet it's still true: FIs can outsource activities, but they can't outsource responsibility for those activities. That means an FI will be held accountable if third parties violate laws or regulations. Appendix E tells examiners that "with respect to compliance risk…determine whether management identified risks associated with the use of nontraditional third-party service providers often found in the innovation and devel opment sphere of MFS."

Reputation Risk

Participating in MFS means sharing data with third-party providers and that makes privacy and data security potential risks. That's why Appendix E's examiner objectives include assessing whether management identifies "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."

Measuring Risk

It's not enough to identify risks. FIs must have systems in place to measure the level and type of risks that mobile financial services present. This way management can gauge which risks present the greatest threat and which controls will be most effective and thus, most worthy of resources.

Taking a page from the FFIEC Outsourcing IT Handbook, there should be:

- Objective measurements for each significant element
- Required measurement reporting
- Benchmarks defining when measurements fall short of expectations

Appendix E emphasizes that "This process should be ongoing and updated whenever management implements a change to the strategy or MFS."

Mitigating Risk

FIs need to find a way to work effectively with a broad range of MFS-related parties to ensure laws and regulations are followed and that sensitive data is kept private. This is best accomplished by developing policies and procedures to ensure compliance as part of the strategic planning process—and then selecting and collecting internal controls to ensure those policies and procedures are being followed.

Appendix E provides a great amount of detail when it comes to operational controls, suggesting that banks have controls related to enrollment; authentication and authorization; application development and distribution; application security; customer awareness; and logging and monitoring. Most critical of all from a vendor management perspective, the FFIEC also includes contracts as an important operational control to consider.

[3] Financial Institution Letter: FDIC Guidance for Managing Third-Party Risk https://www.fdic.gov/news/news/financial/2008/fil08044a.html

"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."

Most critical of all from a vendor management perspective, the FFIEC also includes contracts as an important operational control to consider.

Leveraging Contracts to Mitigate Risk

Appendix E doesn't go into the specifics of constructing a strong contract, but other guidance has told us that a well-written contract clearly defines the roles and responsibilities of both the FI and third-party. In its Vendor Management Technical Video-Outsourcing Technology Services based on the FFIEC IT Booklet "Outsourcing Technology Services," the FDIC calls contracts the most important control in the vendor management process. Elements to consider include:

- Scope of service
- Security and confidentiality
- Internal controls
- Audit
- Reports
- Business resumption/ contingency plans
- Sub-contracting
- Regulatory compliance
- Performance standards

This also includes service-level agreements, or SLAs, that guarantee vendor performance. SLAs outline minimum performance standards during the term of a contract—and the potential consequences for failing to meet those standards. It measurably and specifically describes an institution's expectations for mobile products and services, everything from monitoring to the frequency of penetration testing. Then it creates accountability with financial penalties or even an exit strategy in event the vendor breaches the agreement.

Appendix E specifically mentions several suggested controls for third-party providers, saying FIs need should "encourage" mobile-payments platform developers to use:

- Traffic filtering to help prevent or minimize denial-of-service attacks.
- Trusted platform modules.
- Secure telecommunications protocols (e.g., secure sockets layer/transport layer security [SSL/TLS]).
- Tokenization 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.

Other third-party controls specifically recommended by Appendix E include:

- Require[ing] website developers to follow a secure development life cycle to increase the security of the websites designed for the financial institution.
- Require[ing] developers to build a secure website 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.

It also recommends strong controls over customer information access by mobile-platform providers. When it comes to reputation risk, "Examiners will look to see use of controls to minimize or prevent disclosure of personal information and the potential for fraudulent transactions" and "review management's mitigation of risks associated with the use of a third party, if applicable."

Monitoring and Reporting

Risk is not a static issue. New risks are constantly emerging. Meanwhile FIs must regularly assess the effectiveness of its controls to limit known risk.

That's why Appendix E says that every FI needs systems in place to determine if mobile products and services are performing as expected. These systems should specifically:

- 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.

Practically speaking, this means that FIs should conduct regular, ongoing monitoring, studying both "point-in-time and trend activity" to assess third-party vendor performance and risk management. If events in the outside world are changing the potential for risk, FIs must be sure third parties are keeping up. It's also critical to know if third parties are doing everything they promised to ensure compliance, security and privacy standards are being met.

This is one place where a strong contract, including SLAs, can assist an FI. The contract should require third parties to provide regular reports and audits demonstrating third party performance. FIs need to stay on top of collecting and examining these documents and the board and management must use this information to conduct continual risk assessment. Regular monitoring and reporting allows an FI to manage risk fluidly—and even decide if it's necessary to stop providing a specific MFS due to unacceptable levels of risk.

Practically speaking, this means that FIs should conduct regular, ongoing monitoring, studying both "point-in-time and trend activity" to assess third-party vendor performance and risk management.

Conclusion

As mobile financial services continue to expand and FIs feel competitive pressure to launch innovative and convenient products, risk will remain an important part of the discussion. Before FIs can go toe-to-toe with nonfinancial competitors seeking to snatch away market share, they need to embrace a comprehensive approach to enterprise risk management that goes beyond the technological aspects of MFS to carefully identify and assess all aspects of risk—including the compliance and reputational risk created by third-party providers. Measuring and mitigating risk through carefully constructed contracts can limit an FI's potential exposure to harm via third parties while continual monitoring can keep an FI aware of developments in the MFS ecosystem and keep assessments up-to-date.

Proper vendor management has never been more critical.

Ncontracts® is a leading provider of risk management software and services to financial institutions. While we started with our industry-leading vendor management platform, our portfolio offerings have evolved to feature enterprise risk management, business continuity risk management, compliance management, findings management, and cybersecurity management. More than 650 financial organizations use Ncontracts to manage risk more efficiently and effectively using our integrated suite of software and services.

(888) 370-5552
info@ncontracts.com
www.ncontracts.com