Mobile Banking: Rewards and Risks

Mobile banking is a relatively new banking service that is rapidly gaining popularity with consumers and businesses. More than half of the 100 largest banks in the United States offer mobile banking[1] and approximately 19 million U.S. households use this service.[2] Analysts estimate use of mobile banking will continue to grow, potentially expanding to 38 million households by 2015.[3] However, with more widespread use comes the potential for increased fraud that could harm financial institutions and customers.

Mobile banking is the use of a mobile device, commonly a cell phone or tablet computer, to conduct banking activities, such as balance inquiry, account alerts, and bill payment. It is not the same as mobile *payments*, which uses the same mobile devices to initiate payments from a person to other people or businesses. Mobile banking is offered by insured depository institutions while mobile payments systems can be offered by many types of companies.

This article discusses the technologies used to deliver mobile banking services, identifies the potential risks to financial institutions and customers, and describes strategies for mitigating these risks. The information provided in this article represents the informed perspective of the author and is offered as a resource for financial institutions offering mobile banking services to their customers. This article should not be considered supervisory guidance.

Mobile Banking Delivery Channels

Mobile banking is offered through three delivery channels:

- Text messaging/short message service (SMS)
- Mobile-enabled Internet browser
- Mobile applications (apps).

To appeal to a greater number of customers, some financial institutions are finding it advantageous to offer mobile banking through multiple delivery channels. In fact, nineteen of the fifty-four largest banks that offer mobile banking use all three channels and seventeen offer two of the three channels.[4]

SMS-based mobile banking was the first channel that enabled customers to interact with their bank using a mobile device. SMS messages are short, typically limited to 160 characters per message, and can be sent and received by most mobile phones. The financial institution and customer use text messages to exchange financial information and instructions within the parameters set by the bank.

With the advent of smart phones, mobile banking has become more attractive and user friendly. During the past two years, smart phone ownership increased 127 percent.[5] As of July 2011, 34 percent of all consumers owned smart phones.[6] Using a

[1] First Annapolis Consulting, 2010 Mobile Banking and Payments Study (2010) (private study available for a fee) (on file with author).

[2] *Online Banking Report,* no. 188, Jan. 18, 2011, at 5 (private study available for a fee) (on file with author).

[3] *See* id.

[4] *See* First Annapolis Consulting, supra note 1, at 17.

[5] Javelin Strategy and Research, Smartphone Banking Security: Mobile Banking Stalls on Consumer Fears (2011) (private study available for a fee) (on file with author).

[6] *See* id.

smart phone or tablet computer with an embedded browser, customers can visit the institution's online banking Web site from virtually anywhere. This provides customers with an online banking experience similar to what is available on desktop computers.

As smart phones are now capable of running many applications, and portable tablet computers are increasing in popularity, more financial institutions have introduced mobile application-based banking. This form of mobile banking uses a custom-designed software application installed on the customer's mobile device. The application is unique to each device, providing the most user-friendly experience of the three delivery channels. In fact, app-based mobile banking is now the fastest growing delivery channel.[7]

Although use of mobile banking services continues to grow, the *rate* of increase slowed during the past two years due in part to consumer concerns about security. The results of a study conducted by Javelin Strategy and Research, a California-based firm focused on global financial services, show that the number of consumers rating online banking unsafe rose from 26 percent to 40 percent during this time.[8] Security concerns present significant challenges for financial institutions providing mobile banking services, and each delivery channel poses unique risks for institutions and customers.

Channel-Specific Mobile Banking Risks

SMS is considered an unsecure channel because text messages cannot be encrypted, increasing the likelihood that SMS-based mobile banking users may be susceptible to scams. Using a tactic known as "social engineering," fraudsters send text messages that may mislead customers into believing they are communicating with their financial institution and then revealing sensitive bank account information, for example, account number, logon ID, or password.

More secure than SMS, Web-based mobile banking takes advantage of established Internet security protocols, and the service can be used on mobile devices with wireless Internet access. However, mobile browsers displayed on small screens, particularly smart phones, generally do not display the visual security clues more easily seen on the full-scale browsers of large screens. Thus, customers may miss a visual warning that their online banking session has been compromised.

Mobile application-based banking also is considered more secure than SMS. However, security professionals debate whether this delivery channel is more or less secure than Web-based mobile banking. The development of mobile applications using secure coding techniques may limit the ability of fraudsters to intercept and control a mobile

[7] W.B. King, "Getting Smart – Mobile Banking Continuing to Gain Momentum," Credit Union Business, http://www.creditunionbusiness.com/2011/09/15/getting-smart-mobile-banking-continuing-to-gain-momentum, (last visited October 20, 2011).

[8] *See* Javelin Strategy and Research, *supra* note 5, at 12.

Mobile Banking

continued from pg. 15

banking session or capture sensitive customer information. However, in the rush to get mobile applications to market, secure code review and testing may not be sufficiently robust. Also, mobile banking can be compromised by the installation of rogue, corrupt, or malicious applications on a customer's mobile device.

A recent study looked at the security of four types of mobile applications – financial services, social networking, productivity,[9] and retail.[10] The study focused on the types of sensitive data that mobile applications store on the device and whether these data were stored securely. Each application was rated "Pass," "Warn," or "Fail." A "Pass" rating means sensitive data are not stored on the device or are encrypted. A "Warning" rating means certain data are stored on the device, but this does not put the user at significant risk of fraud. A "Fail" rating indicates sensitive data, such as account numbers and passwords, are stored on the device in clear text, placing the user at an increased risk of identity theft or other financial fraud.

Although the results show a significant share of all four types of applications failed the test, the financial services industry had the largest percentage of apps that passed the test (see table below). These results suggest that even though the financial services industry has more work to do to ensure mobile applications do not store sensitive information unnecessarily or unencrypted, at least for purposes of this study, this sector outperformed the others.[11]

Given the unsecure nature of SMS-based mobile banking, this channel would seem to be much more appropriate for communicating non-sensitive information, which may include confirming transactions initiated through another channel, rather than initiating transactions such as bill payments, funds transfers, or adding new payees. Institutions should make reasonable efforts to migrate customers

Mobile Application Security by Type of Application

Industry	Pass	Warn	Fail
Financial Services	44%	31%	25%
Social Networking	0%	26%	74%
Productivity	9%	49%	43%
Retail	0%	86%	14%

Source: ViaForensics.

[9] Productivity applications are intended to help a user be more productive, for example, allowing the user to access a variety of e-mail accounts from one central application or update a blog while away from his computer.

[10] *Mobile App Security Study: appWatchdog Findings,* viaForensics, http://viaforensics.com/education/white-papers/appwatchdog-findings-mobile-app-security-iphone-android/ (last visited October 18, 2011).

[11] *See* id.

from SMS to more secure Web- or app-based mobile banking platforms. As mobile devices and browsers become more sophisticated, financial institutions should use the advances to improve the security of Web-based mobile banking. The goal should be to make Web-based mobile banking as secure as online banking from a customer's personal computer.

As is the case with any banking product or service involving a third-party provider, financial institutions that offer app-based mobile banking are expected to work with reliable, knowledgeable, and reputable vendors to develop applications using secure coding techniques. Appropriate steps should be taken in coding and testing to ensure the application does not contain exploitable weaknesses. Perhaps most importantly, institutions should distribute applications and updates securely and make reasonable efforts to educate customers that banking applications should be downloaded from reputable sources, such as the institution's Web site or other designated download sites. When vulnerabilities are discovered, the financial institution has an obligation to promptly develop and deploy security patches.

Other Mobile Banking Risks

In addition to the risks specific to delivery channels, financial institutions should consider the following risks and vulnerabilities when offering mobile banking services to their customers:

Secure authentication of mobile customers

The portability of mobile devices enhances their usefulness; however, it also means these devices are susceptible to being lost or stolen. To mitigate this risk, financial institutions should implement controls to verify the person accessing the mobile banking service is the customer. The Federal Financial Institutions Examination Council (FFIEC) recently issued supervisory guidance on strong customer authentication that applies to mobile banking.[12] Possession of the mobile device alone should not be enough to permit access to the mobile banking application. At the very least, access to the device should be password protected and users seeking access to the mobile banking service should be subject to strong authentication as described in the FFIEC guidance.

[12] FIL-50-2011, "FFIEC Supplement to Authentication in an Internet Banking Environment" (June 29, 2011) at http://www.fdic.gov/news/news/financial/2011/fil11050.html; *see also* FIL-103-2005, "FFIEC Guidance on Authentication in an Internet Banking Environment" (October 12, 2005) at http://www.fdic.gov/news/news/financial/2005/fil10305.html.

Mobile Banking

continued from pg. 17

Mobile malware and viruses

To date, problems involving viruses and malware targeted at mobile devices have been limited; however, the ubiquity of mobile devices, common operating systems, and downloadable applications make them a prime target. The market for mobile antivirus and malware detection security software is continuing to evolve. Financial institutions should monitor these developments and consider when to recommend mobile banking customers run security software on their devices, including whether the institution should make the software available directly to customers.

Data transmission security

Mobile devices generally are designed to accept instructions from cell towers and search for the strongest cell tower signal. Mobile devices must authenticate themselves to the cell tower using the unique information on the device's subscriber identity module (SIM) card to show it is a legitimate device. However, cell towers are not required to provide similar authentication to mobile devices. Telecommunications standards and mobile devices are designed to be backward compatible; if the cell tower operates on an older standard (e.g., 2G instead of 3G or 4G), the mobile device will adopt the less secure standard to complete the wireless connection. Therefore, it is possible to build and operate a rogue cell phone tower, trick mobile devices into connecting to the rogue tower, and hijack the mobile session, potentially compromising mobile banking sessions.

In addition, most mobile devices can connect to wireless local area networks (WLANs) used by many customers to minimize telecommunications expenses and optimize connection speeds. However, financial institutions should caution customers against using public WLANs for mobile banking. Neither the customer nor the financial institution can ensure a public WLAN is secure, and incidents have occurred where banking credentials were stolen from an unsecure WLAN.

Compliance risk

Compliance risk often arises from violations of laws or regulations, financial institutions operating inconsistently with supervisory guidance, or institutions' noncompliance with internal policies, procedures, or business standards. Generally, the consumer laws, regulations, and supervisory guidance that apply to traditional financial services delivery channels also apply to services provided to consumers through mobile banking.

However, the relevant laws, regulations, and guidance will apply differently, depending on how a financial institution is involved in mobile banking. Financial institutions that enable consumers to access deposit and loan services through their mobile device should ensure that any applicable disclosure requirements, including format, content, timing, and manner of delivery, are fully accessible to the customer. In addition, institutions using the mobile banking channel to provide information about products and services to consumers should verify compliance with applicable advertising rules and regulations. For example, banks advertising credit products subject to the Fair Housing Act are required to display the Equal Housing Lender logo and legend. Institutions advertising deposit products and services are required to comply with Regulation DD advertising disclosures and, if relevant, display the official advertising statement found in the FDIC's regulations.

The rapid pace of development in mobile financial services will require that compliance officers, manage-

ment, and system designers work closely together to effectively use the new technology while assessing, identifying and controlling for compliance risks.[13] Therefore, a financial institution should broadly consider the impact of its mobile banking strategy on operations and take steps to ensure the compliance management system addresses the types and level of mobile banking technology used by the institution.

Regulatory Considerations

Although mobile banking is a relatively new service, many associated risks are present in other banking technologies and services. Financial institutions should review other regulations and supervisory guidance issued by the federal banking agencies, such as the *FFIEC IT Examination Handbooks on Development and Acquisition, Outsourcing Technology Service Providers, E-Banking,* and *Information Security.*[14]

Institutions should also review the following regulations and supervisory guidance:

- *Interagency Information Security Standards*[15]
- *Interagency Regulations and Guidelines on Identity Theft Red Flags*[16]
- *FFIEC Guidance on Risk Management of Remote Deposit Capture*[17]
- *Guidance on Electronic Financial Services and Consumer Compliance*[18]
- *Guidance for Managing Third-Party Risk*[19]

This body of supervisory guidance addresses steps financial institutions are expected to take to protect sensitive customer information, prevent identity theft, enable secure online transactions, communicate appropriate consumer disclosures, and manage the risks associated with the use of third-party service providers.

[13] The examples in this section are provided for illustration and do not constitute a complete list of mobile banking capabilities or consumer compliance matters associated with this delivery channel.

[14] FFIEC IT Examination HandBook InfoBase, http://ithandbook.ffiec.gov/it-booklets.aspx.

[15] 12 CFR § 364, Appendix B.

[16] FIL-100-2007, "Interagency Regulations and Guidelines on Identity Theft" (November 15, 2007) at http://www.fdic.gov/news/news/financial/2007/fil07100.html.

[17] FIL-4-2009, "FFIEC Guidance on Risk Management of Remote Deposit Capture" (January 14, 2009) at http://www.fdic.gov/news/news/financial/2009/fil09004.html.

[18] FIL-79-98, "Guidance on Electronic Financial Services and Consumer Compliance" (July 16, 1998) at http://www.fdic.gov/news/news/financial/1998/fil9879.html.

[19] FIL-44-2008, "Guidance for Managing Third-Party Risk" (June 6, 2008) at http://www.fdic.gov/news/news/financial/2008/fil08044.html.

Mobile Banking

continued from pg. 19

As the demand for mobile banking services continues to grow, financial institutions should conduct a comprehensive risk assessment or update existing assessments during the design, testing, and implementation of a mobile banking product. Guidance for performing an effective risk assessment is available in the *FFIEC IT Examination Handbook on Management.*[20] Risk assessments should be updated in response to changes in technology, business strategy, security threats, product functionality, and legal requirements. Should a risk assessment identify new risks or vulnerabilities, financial institutions should address them promptly to appropriately and effectively mitigate the risks for the institution and its customers.

Conclusion

With greater use of all types of mobile services, mobile banking is expected to continue to grow. Mobile banking provides greater convenience for customers as it allows them to accomplish tasks "on the go." However, this service is not without risks. Financial institutions are challenged to ensure their mobile banking service is designed and offered in a secure manner, and customers are made aware of steps they can take to protect the integrity of their mobile banking transactions.

Jeffrey M. Kopchik
Senior Policy Analyst
jkopchik@fdic.gov

[20] FFIEC, IT Examination Handbook on Management 15-24 (June 2004) available at http://ithandbook.ffiec.gov/it-booklets/management.aspx; *see also* FFIEC, *supra* note 10; *see also* Paul M. Onischuk, "*Customer Information Risk Assessments: Moving Toward Enterprise-wide Assessments of Business Risk,*" ***Supervisory Insights*** (Winter 2009) at http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin09/si_win09.pdf.