Bloomberg Law Reports® Banking & Finance

Mobile Banking: What Banks Need To Know When Outsourcing Their Platforms

Timothy R. McTaggart and David W. Freese, Pepper Hamilton LLP

Introduction

The mobile phone is transforming the banking industry. The online banking platforms established over a decade ago freed customers from brick-and-mortar branches, allowing them to execute transactions at any time. Mobile banking is the next step in this bricks-to-clicks evolution, allowing customers to execute transactions from anywhere. By 2013, an estimated 53 million consumers will bank by mobile phone, representing nearly 52 percent in annual compound growth from 2009.[1]

As mobile banking-capable phones have gained in popularity with consumers,[2] so has mobile banking platform adoption with financial institutions. Most large U.S. banks currently offer some combination of the following mobile banking services to their customers:

- account balance inquiries and statements;
- bill payment;
- funds transfers;
- branch and ATM locaters; and
- mortgage alerts.

Banks typically offer these services through three main channels. First, Short Messaging Service (SMS) technology allows financial institutions to send text messages that can, for example, notify customers of their account balance or the nearest ATM location. Second, Wireless Application Protocol (WAP) allows customers to access a bank's mobile banking website via a phone's Internet browser. Banks also may offer Mobile Client Applications (MCAs) that allow customers to download mobile banking software directly onto their phones.

However, financial institutions do not offer mobile banking services in isolation. They typically do not have the technical resources or specialized knowledge to develop mobile banking platforms. Consequently, financial institutions outsource this process to mobile banking vendors (Vendors) who provide them the technology that runs the platforms. This article discusses issues financial institutions must consider and resolve when contracting with Vendors to establish their mobile banking platforms.

Issue 1: Developing Enterprise-Wide Risk Management Processes

Financial institutions are required to develop risk management processes to manage their relationships with information technology vendors, including Vendors.[3] Outsourcing mobile banking functions increases operational risk, which arises "from fraud, error, or the inability to deliver products or services."[4] Vendor risk management processes should be designed to identify, measure, monitor, and control these operational risks.

In terms of identifying risks, mobile banking is still in its infancy, which gives rise to strategic risk: the risk that a financial institution's management may not understand mobile banking functions and therefore will not be able to control the related risks. The Vendor-financial institution relationship also gives rise to legal risk, or the risk that the Vendor will fail to comply with legal or regulatory requirements, which would subject the financial institution to penalties. Outsourcing mobile banking functions also subjects financial institutions to reputational risks for errors that occur outside of their control. If customers lose access to their mobile banking functions due to system error, they likely will blame the financial institution whose name they associate with the platform, not a Vendor who is not known to them.

When developing procedures to measure the risk associated with a Vendor, a financial institution first should look to the risks associated with its intended use of mobile banking services. The procedures should determine how critical mobile banking is to the financial institution's business: the more critical, the greater degree of risk. Further, if the financial institution expects a great number of mobile banking transactions, it should assign the function a greater degree of risk. A financial institution's risk management procedures also should measure the risk associated with specific Vendors. The procedures should be designed to assess, among other things, a Vendor's experience, financial strength, employee turnover and business continuity plan. Since most Vendors are still relatively young companies, this measurement becomes even more vital.

Monitoring the risks associated with a Vendor relationship is an important part of a financial institution's risk management procedures. The program should be designed to ensure quality of service by monitoring the Vendor's controls and financial condition. With respect to monitoring controls, a financial institution should evaluate a Vendor's internal and external audits and any SAS 70 reports.[5] Financial institutions should also dedicate personnel to trace transactions, such as mobile bill payments, to ensure the Vendor keeps an adequate audit trail and to spot-check the Vendor's calculations, such as mobile balance transfer calculations. With respect to monitoring a Vendor's financial condition, a financial institution should evaluate a Vendor's periodic financial statements and any independent auditor reports. Many Vendors have been in business for less than a decade, so examining their financial viability is critical.

Importantly, the information technology services that financial institutions outsource are subject to regulation and examination to the same extent as if financial institutions performed the services themselves.[6] Vendors are not excepted. Banking regulators identify Vendors that warrant examination based on the level of risk their services pose to a financial institution. This is important to the financial institution because if an examination shows a Vendor has weak risk management controls, the financial institution may have to take corrective action because it is ultimately responsible for managing its own risks. Therefore, when deciding which Vendor to choose, a financial institution should confirm the appropriateness of a Vendor's risk management systems, such as its data security, customer verification and privacy processes. It should also inquire as to whether the Vendor has ever been examined by a federal banking regulator and request a copy of the examination report. After choosing a Vendor, the financial institution should conduct ongoing monitoring of the Vendor's service-level reports, audits, and internal control testing results. This added due diligence and monitoring will reduce the possibility that the financial institution will eventually have to answer to regulators for its Vendor's risk management shortcomings.

Issue 2: Data Security

Security breaches of mobile financial data can come in many forms. Hackers can upload malware onto a customer's mobile phone that allows access to data. Thieves can attempt to hijack data from a lost or

stolen phone. SMiShing, the mobile equivalent of email phishing, lures customers into providing financial data via text message. Further, text messages present different threats than mobile web, which presents different threats than mobile applications. Customers are aware of these dangers and their unease over mobile banking security is a primary cause for slower adoption.[7]

When choosing a Vendor, a financial institution must consider its obligations under the Gramm-Leach-Bliley Act (GLB Act)[8] and the Interagency Guidelines Establishing Information Security Standards (Guidelines)[9] published under it by the federal banking regulators. The GLB Act and the Guidelines require financial institutions to develop, monitor and adjust safeguards to protect the security, confidentiality, and integrity of customer information. A financial institution must integrate its mobile banking operations into its GLB Act security program and should choose a Vendor whose security solutions ease this integration. For example, a financial institution should reevaluate its fraud prevention and tracking procedures in light of SMiShing and consider whether a Vendor's anti-SMiShing solutions, such as the use of account nicknames, meet the requirements of those procedures.

Customers, however, also may view too many security features as inconvenient. Vendors therefore often give financial institutions options on which security components to offer. For example, a Vendor may give a financial institution the opportunity to offer both balance inquiry and fund transfers via text messaging. Since text messaging generally is less secure than mobile web or mobile applications, the financial institution must decide whether to offer only balance inquiries (erring on the side of security) or offer both (erring on the side of convenience). Vendors also may give financial institutions options for back-end operations. For example, a Vendor may give the option of either preserving encrypted message data or not preserving it to lessen the risk of it being hacked later.

A financial institution considering different security options offered by Vendors must keep its obligations under the GLB Act and the Guidelines in mind when making its decision. When integrating its decision to allow fund transfers via text messaging into its safeguarding program, for example, a financial institution continuously must download new security patches and monitor whether the fund transfers compromise customer information. If it eventually determines that allowing fund transfers via text messaging compromises the data, it should drop the option and proceed with the balance inquiry-only model.

Issue 3: Anti-Money Laundering

Mobile banking presents new opportunities for criminals to launder money and finance terrorism. Money launderers and terrorist financiers may gain access to a mobile banking account by stealing a mobile phone with inadequate security features, by hacking a wireless network transferring mobile financial data, or when an authorized account holder purposefully provides them access.[10] The international portability of mobile phones only increases these risks.

The United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,[11] or the USA PATRIOT Act, imposes on financial institutions various requirements designed to prevent terrorists from accessing financing. Financial institutions must, *inter alia*, develop policies and procedures to detect and prevent money laundering and submit suspicious activity reports on transactions suspected of laundering money through such institutions.[12] Given the increased risks that mobile banking poses, it is essential that financial institutions integrate their mobile banking operations into their anti-money laundering (AML) policies and procedures.

Vendors contribute most directly to a financial institution's AML process by providing customer authentication solutions. It is critical that a financial

institution determine the adequacy of a Vendor's authentication system. Multi-factor authentication is the minimum legal standard,[13] where the first factor to authenticate the phone's authorized user is something she "has" and the second factor is something she "knows." An authorized transaction will consist of the user initiating the transaction through the phone she registered with the financial institution when signing up for the program (*i.e.*, the thing she has) and confirming the transaction with a PIN or password (*i.e.*, the thing she knows).

Financial institutions should consider opting for solutions that exceed the minimum. Some Vendors offer "out-of-band" authentication, where the platform uses two separate channels simultaneously to verify a user. For example, if a customer authorizes a transaction via mobile web, the platform would send a text message requesting a PIN or instruct a customer service representative to call the phone and request the user verbally provide additional information. Certain Vendors also offer a feature to send alerts to a customers to verify large transactions within a predetermined timeframe before the transaction is completed. These added features may not be necessary for all transactions, but a financial institution should determine the higher risk transactions (*e.g.*, those above a certain dollar value) that qualify for this treatment.

In addition to choosing the proper authentication solution, a financial institution must integrate the Vendor's solution into its existing AML software. Depending on the financial institution, that software may cover retail banking, commercial banking, private banking, and securities transactions. A financial institution should inquire whether its Vendor offers AML-specific programs such as currency transaction report creation, suspicious activity monitoring, or Office of Foreign Assets Control screening, and if so, how it can be integrated into its existing AML software. If the Vendor does not offer such programs, the financial institution should contact its existing AML software Vendor to determine whether that Vendor can meet its mobile banking AML needs.

Issue 4: Electronic Fund Transfer Act and Regulation E Issues

Financial institutions, far more than any other stakeholder in mobile banking transactions, are legally obligated to ensure that a mobile banking transaction is completed correctly. The Electronic Fund Transfer Act (EFT Act),[14] and Regulation E[15] adopted under it by the Board of Governors of the Federal Reserve System (Federal Reserve Board), govern electronic fund transfers (EFTs) to and from a customer's account held by a financial institution. EFTs are transfers of funds initiated by electronic means, including ATM transfers, debit card transactions, direct deposits and withdrawals, telephone-initiated transfers and online bill payments. Although the Federal Reserve Board has been silent on the issue, mobile banking transactions are likely covered under the EFT Act and Regulation E.

The EFT Act holds a financial institution liable for damages caused by its "failure to make an electronic fund transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner when properly instructed to do so by the consumer."[16] The nature of banking through a mobile phone presents new opportunities for transaction disruption, such as wireless service being dropped mid-transaction and mobile hackers interfering with wireless networks. A transaction also could be disrupted due to a technical failure of the Vendor's platform, for example a mobile client application failing before a transaction is completed. As such, financial institutions need to be especially mindful of their EFT Act and Regulation E obligations when negotiating services contracts with Vendors. During negotiations, particular attention should be paid to indemnification provisions. A financial institution should consider requesting that the vendor indemnify it for any losses outside of the financial institution's control that it incurs as a result of the failure of the Vendor's platform to complete a transaction. Relatedly, the financial institution should disclose to its customers in its mobile banking disclosure document that it disclaims all

liability in the event that a vendor-related or wireless service-related event outside of its control causes a transaction failure.

Financial institutions also must be mindful of their liabilities under the provisions of Regulation E that protect customers from losses caused by unauthorized EFTs. Regulation E limits a customer's liability for an unauthorized EFT to $50 if he or she notifies the financial institution within two days after learning of it or to $500 if the customer notifies the financial institution after two days. Regulation E therefore places greater liability on financial institutions for unauthorized EFTs than Regulation Z places on financial institutions for unauthorized credit card transactions. Regulation Z does not have a tiered $50 or $500 consumer liability limit, instead limiting consumer liability for unauthorized credit card transactions to $50.[17]

Consumer advocates, however, have argued that the advent of mobile banking and mobile payment technologies presents a unique opportunity for regulators to bring Regulation E's $50 or $500 liability limitations into harmony with Regulation Z's $50 liability limitation for unauthorized credit card transactions.[18] They argue that such a change would provide consumers with consistent protection across product lines and reduce consumer confusion. Consumer advocates also have pressed financial institutions to adopt voluntary zero liability policies with respect to customers' liability for unauthorized mobile banking EFTs.[19]

In response, some financial institutions voluntarily have adopted zero liability policies for their mobile banking customers.[20] If a financial institution chooses to adopt such a policy, it becomes especially important to scrutinize a Vendor's data security and customer authentication solutions. This added due diligence may help decrease the number of reimbursements for unauthorized EFTs and their negative effect on mobile banking margins.

Conclusion

Vendors are not subject to the vast array of banking laws and regulations as are financial institutions. Mobile banking also presents new security, AML and operational issues for financial institutions. Financial institutions therefore should understand that when they contract with a Vendor to provide mobile banking services, they must independently determine that they will comply with all applicable laws and regulations. They also should consider how the services offered by the Vendor will integrate into their existing policies and procedures and software, including their security procedures, AML software, and Regulation E disclosures. With appropriate attention paid to regulatory compliance, financial institutions and Vendors can forge lasting, profitable relationships while providing customers an exciting new banking product long into future.

Mr. McTaggart is a partner and Mr. Freese is an associate in the Financial Services Practice Group of Pepper Hamilton LLP. This article contains information for general purposes only and does not constitute the provisions of legal advice. Readers should consult with competent counsel in connection with any of the issues raised within this article.

---

[1] TowerGroup, *Mobile Banking Hits Mainstream in 2009* (May 26, 2009), http://www.towergroup.com/research/news/news.htm?newsId=5360.

[2] Roger Entner, *Smartphones to Overtake Feature Phones in U.S. by 2011* (March 26, 2010), http://blog.nielsen.com/nielsenwire/consumer/smartphones-to-overtake-feature-phones-in-u-s-by-2011/.

[3] Federal Financial Institutions Examination Council, *Outsourcing Technology Services — IT Examination Handbook* (June 2004), http://www.ffiec.gov/ffiecinfobase/html_pages/outsource_book_frame.htm.

[4] *Id.* at 6.

[5] The Statement on Auditing Standards No. 70: Service Organizations, more commonly known as a SAS 70 report, is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants that provides guidance to auditors

when assessing the internal controls of a service organization and issuing an auditor's report.

[6] 12 U.S.C. § 1867(c)(1) (2006); 12 U.S.C. § 1464(d)(7) (2006).

[7] ClairMail, *Mobile Security: Four-Point Strategy for Secure Mobile Banking and Payments* at 3 (Jan. 2010).

[8] Pub. L. 106–102, codified at 15 U.S.C. §§ 6801-6809.

[9] 12 C.F.R. Pt. 30.

[10] Pierre-Laurent Chaiten, et al., *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks from Money Laundering and Terrorist Financing*, World Bank Working Paper No. 146, at 22 (2008). In Brazil, for example, law enforcement is seeing a surge in so-called "orange accounts," where criminals pay the impoverished to open and provide them access to mobile banking accounts. *Id.*

[11] Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the U.S.C.).

[12] Money services businesses (MSBs), such as money transmitters, also are subject to the PATRIOT Act's anti-money laundering (AML) requirements. Some third parties in the mobile banking and mobile payments arena, such as PayPal, have registered under the laws of certain states as MSBs. It is prudent for a financial institution to ask a mobile banking vendor whether it has registered with any state as an MSB, and if so, review the vendor's AML policies and procedures. The Financial Crimes Enforcement Network (FinCEN), the agency within the Treasury Department responsible for combating financial crimes, recently proposed to increase the AML requirements of certain financial institutions and MSBs. On September 27, 2010, FinCEN issued a Notice of Proposed Rulemaking that would, among other things, require financial institutions engaging in international wire transfers to submit to it the related money transmittal orders, regardless of the quantity of funds wired. MSBs would have to submit money transmittal orders for international wire transfers valued at $1,000 or more. Currently, financial institutions need only retain records for transfers of $3,000 or more and need only report suspicious wire transfers. *Cross-Border Electronic Transmittals of Funds*, 75 Fed. Reg. 60377 (Sept. 30, 2010).

[13] Federal Financial Institutions Examination Council, *Authentication in an Internet Banking Environment* (Oct. 12, 2005), http://www.ffiec.gov/pdf/authentication_guidance.pdf.

[14] 15 U.S.C. § 1693, *et seq.*

[15] 12 C.F.R. pt. 205.

[16] 15 U.S.C. § 1693h(a)(1).

[17] 12 C.F.R. § 226.12.

[18] *See, e.g.*, Mark McCarthy and Gail Hillebrand, *Viewpoint: Mobile Payments Call for Clear Consumer Protections*, Am. Banker (Aug. 10, 2010), http://www.americanbanker.com/issues/175_152/vp-hillebrand-mobile-protections-1023818-1.html?zkPrintable=true (arguing that regardless "of the technology or business organization involved, the same high level of consumer protections should be guaranteed by law and contract for any payment service.").

[19] *Id.*

[20] For example, SunTrust has adopted a policy that covers consumers for any unauthorized EFTs, including loss of interest, insufficient funds, and overdraft charges, if they report the EFT within 60 days of receiving the statement containing the EFT. SunTrust, *Mobile Banking*, https://www.suntrust.com/portal/server.pt/community/mobile_banking/1783.