

Mitigating the risk in mobile banking

By Luke Nordlie and Hicham Chahine, Crowe Horwath LLP

Consumer adoption of mobile devices such as smartphones and tablets represents a tantalizing opportunity for banks to lure customers through mobile-banking applications. However, before offering these services, executives should conduct a thorough risk assessment of the technology involved. By taking a comprehensive approach to managing the risks of mobile banking, banks not only can safeguard their operations but also can pursue new customer segments without exposing themselves to unnecessary risk.

Over the past decade, mobile phone penetration among consumers has increased dramatically, and it continues to grow. According to a survey by the Federal Reserve, 87% of the U.S. population now has a mobile phone. A Pew Internet & American Life Project report says that nearly half of those are smartphones (meaning they can connect to the Internet) and that almost one in five people owns a tablet computer such as the iPad.

Consumers have become accustomed to using these devices for a range of banking transactions. Most use mobile banking to check account balances, but 42% of consumers also use their mobile devices to transfer money between their own related accounts. The Fed survey found that 21% of smartphone users engaged in some form of mobile banking in the past year, and an additional 11% said they intended to do so in the next year.

In a highly competitive market, mobile banking can be a differentiator. Banks understandably do not want to miss out on a rapidly growing new market of consumers who value flexibility and convenience. The market is especially attractive because early adopters tend to be relatively young, tech-savvy, and relatively well off—just the sort of customers that financial institutions want to enroll and keep.

At the same time, according to the Fed's survey report, because mobile phone use is especially prevalent among "young individuals, minorities, and low-income families—groups most likely to be unbanked or underbanked—there is potential for mobile financial services to help integrate these individuals into the financial mainstream" and increase banks' customer base.

Although almost all U.S. banks have established an online banking presence—and therefore might believe they are well prepared to manage the risks of emerging technologies—mobile banking comes with its own challenges. Indeed, financial institutions must understand that the security, privacy, and other risks from mobile devices are more complex and varied than online banking risks. Moreover, some institutions are rushing to develop and launch mobile-banking platforms without fully understanding the security features the applications need to protect their bank and consumers

from fraud.

To add to the challenge, technological advancements are outpacing the ability of regulatory agencies to issue guidance in a timely manner. The Federal Financial Institutions Examination Council continuously updates its regulations and recommendations for standard Internet banking. However, it's still working on mobile guidelines, including security guidelines, leaving software developers guessing about the features to integrate in order to support compliance. Mobile-banking devices that lack high-level multifactor authentication-the need for more than one form of authentication (such as a user ID and a password) to verify the legitimacy of a transaction-will almost certainly become both security and compliance risks.

The risk assessment and management process is therefore an important way in which banks can mitigate the regulatory and compliance risk associated with mobile devices and their software and applications. A bank may remain in compliance by telling the FFIEC how it has evaluated the risks posed by this new generation of mobile software, explain the risks it has identified, and describe how it has decided those risks were acceptable.

Across the banking industry, technology has become interwoven into every facet of operations. An effective risk management program for mobile banking, then, will extend far beyond the most obvious need for thorough technological evaluations to encompass the entire organization. Accordingly, a comprehensive program should include six types of risk and develop appropriate response strategies and programs:

Operational risk-Includes loss from inadequate or failed processes, people, and systems. It usually also includes the threat from potential fraud or theft.

Strategic risk-The impact on earnings of poor decisions, the improper implementation of strategy, and an institution's inability to respond to industry changes or meet customer needs.

Legal risk-Encompasses the potential impact of lawsuits, unenforceable contracts, or adverse judgments. It requires considering potential problems resulting from ambiguous or untested laws, rules, and regulations.

External risk-The possible impact of factors beyond management's control, including new legislation, natural disasters, and certain macroeconomic developments such as supply chain disruptions.

Reputation risk-Includes the impact that any negative developments may have on company stakeholders, from customers and shareholders to regulators and vendors.

Compliance risk-The impact of violations of law or noncompliance with industry rules and regulations or ethical standards.

This comprehensive assessment and management framework allows executives and line operators alike to identify vulnerabilities and craft mitigation strategies. An institution's strategic planning function, for instance, will examine questions such as how fast it intends to develop its mobile device programs. Operations management would look at how well devices and the necessary software and applications actually work and develop rapid response programs in the event of system errors or failures.

In some cases, these efforts might necessitate a rapid response program-for example, in the event of a system failure or software crash. In others, a bank will have to acknowledge vulnerabilities and their potential consequences and accept them as a cost of doing business. In any event, a comprehensive program should establish effective internal controls, including clear executive and line-operator authority that defines who is in charge of responding to risks under different circumstances.

Risk management enables financial institutions to do far more than deal with potential crises. It also allows executives to determine when to take on more risk, how to synchronize that risk with overall business strategy, and how to tap new markets in the face of identified risk.

Assessing and managing mobile device risk effectively, therefore, has the potential to increase market share and profitability. The stakes are high, so banks must commit the necessary time and resources to getting it right.

Contact Information

Luke Nordlie is with Crowe Horwath LLP in the New York office. Hicham Chahine is a principal with Crowe Horwath LLP in the Columbus, Ohio, office.

[This article was posted on September 18, 2012, on the website of ABA Banking Journal, www.ababj.com.]