Mobile Banking Legal Considerations

by Justin B. Hosie and G. Clinton Heyworth
Chambliss, Bahner & Stophel, P.C.

Allowing consumers to access banking networks using a cell phone or similar mobile device can greatly increase various security, and compliance risks. As a result, before implementing a mobile banking program, banks should thoroughly review the legal risks.

Unique Risks Mandate Additional Due Diligence

When a customer sends information from a mobile device over a wireless network, this type of transfer presents transaction risks to the information's integrity and confidentiality. As a result, offering mobile banking requires establishing secure paths into and out of the customer's account.

Since wireless security standards are constantly changing, the Federal Financial Institutions Examination Council IT Examination Handbook, Retail Payment Systems Booklet ("FFIEC Guidance"), advises banks to "exercise extra diligence" in decisions related to wireless solutions and service providers.

Various risks justify the FFIEC's heightened concern. For mobile banking, the inability to see a customer can compound the usual physical security risks. In addition, the parties must consider the fact that wireless signals and hacking can occur. Likewise, the fact that devices can be lost or stolen creates security issues. Each of the following concerns represents a risk unique to Mobile Banking:

1) User ID / Password authentication
2) The device's physical security
3) The device's application security
4) Service provider authentication
5) Data transmission encryption
6) Data storage transmission[1]
7) Unauthorized use and customer liability

Legal Considerations: Regulatory Compliance

All banking laws and regulations potentially apply to wireless banking. However these rules do not fully contemplate mobile payment systems. In the same way that banks updated legal processes for the transition from storefront to electronic banking, a similar transition is required for wireless banking.

For example, the Gramm-Leach-Bliley Act and Regulation P, banks must safeguard customer information. In addition to data storage requirements implemented in branches, banks must maintain effective controls to safeguard data during transmission in the wireless banking process. Moreover, banks using wireless service providers must "ensure that they employ effective risk management practices," according to the FFIEC Guidance.

Likewise, depending on the wireless services offered, banks may risk liability under the Electronic Fund Transfer Act and Regulation E related to unauthorized wireless banking activities. For example, if a wrongful user obtains a consumer's device with a stored password, the FFIEC suggests that the situation "would be similar to losing an ATM or debit card with a personal identification number written on it." ⇨

Banks should also consider compliance with the E-SIGN Act and UETA. The FFIEC Guidance notes that all federal disclosure requirements apply to wireless transactions, and warns that the small screen size limits a banks "ability to deliver meaningful disclosures to customers." Moreover, under the E-Sign Act, if wireless devices cannot store disclosures, then this situation "may affect the institution's consumer compliance disclosure obligations."

Likewise, mobile banking also leads to concerns about the financial system as a whole. The Bank Secrecy Act and Office of Foreign Asset Control requirements mandate that financial institutions implement safeguards to guard against using the financial system as a weapon for terror.

Other Liability Issues

In addition to regulatory concerns, other legal issues to consider involve customer liability based on fraudulent use, and the banks potential liability for missed payments.

Unauthorized Use: Banks must work to prevent unauthorized users from accessing customer accounts either through traditional identity theft (i.e. appropriating passwords and mobile payment devices physically), or through hacking techniques.

Unauthorized account access increases in wireless banking because devices can easily fall into the wrong hands, and because it is difficult for banks to authenticate a mobile consumer's identity. Moreover, mobile devices are easier to lose than traditional PCs. One best practice to reduce unauthorized use is to implement a three-factor security policy. This involves allowing access based on (1) something in the authorized user's possession, (2) something the authorized user knows, and (3) something the authorized user "is." The mobile device satisfies the first requirement, serving as something in the authorized user's possession. Mobile devices are easier to track, and cannot be used to transfer funds without a PIN. A PIN serves as the second factor, something the authorized user knows, thus decreasing the chance of fraud. The third factor of security, "something the user is" is not readily available yet, bio-security will increase security yet again.

Regarding password protection however, one issue specific to wireless banking concerns the fact that customers often use oversimplified passwords, which heightens the risk of misuse. As a result, banks should implement system limitations to prevent oversimplified passwords.

Hacking: Wireless signals may make it easier for hackers to intercept information. As a result, hackers bring a new threat to mobile banking. Recently, hackers focused on Android and MobileMe users. These attacks were quickly countered by Google and Apple respectively, but the concerns linger.[2]

According to the FFIEC Guidance, encryption is essential to wireless banking. Since each consumer's device will transmit data based on an operating system outside the bank's control, banks should clearly disclose such risks to the customer, and work with counsel to properly apportion liability for hacking in such situations. In disclosing risks to consumers, banks should further consider advising their consumers of other sound practices such as using secure PIN codes, downloading mobile apps only from their financial institution, switching Bluetooth off, and avoiding lending their phone to strangers.[3]

Missed Payments: Another key legal issue that sometimes arises concerns situations when a consumer submits a payment, but the device or bank fail to process the payment. As a result, the consumer incurs late or nonpayment fees with a particular service provider. For example, a consumer could direct payment to a utility bill, believe the bank processed the payment, but ultimately have the utilities turned off, because of a mobile processing failure. This can occur when a consumer submits a wireless payment, and the phone enters a "dead zone," unbeknownst to the consumer.

According to the FFIEC Guidance, banks should consider informing customers that "they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services." Likewise, banks should consider affording the consumer an easy method to confirm payments, and work with counsel to properly disclaim liability for such situations.

Conclusion

Currently, few regulations speak to mobile banking liability, security or privacy. However, as systems develop, the mobile banking system should police itself. Statutes and regulations are largely reactive not proactive. Preventing customer loss and insuring compliance with current statutes and regulations may help prevent onerous legislation that may hamper mobile banking.

About the authors

Justin B. Hosie and G. Clinton Heyworth are attorneys at Chambliss, Bahner & Stophel P.C. in Chattanooga, TN <cbslawfirm.com>, (423) 756-3000, consumerfinance@cbslawfirm.com

This article is intended to be informational and does not provide legal advice nor create an attorney-client relationship. Laws are constantly changing, and each federal law, state law, and regulation should be checked by legal counsel for the most current version and before acting on this information. Certification as a Specialist in Consumer Finance Law by the Tennessee Commission on Continuing Legal Education and Specialization is not currently available. None of the attorneys listed in this communication are certified in any area of specialization.

Notes:
(1) See Mobile Banking: Is this Trend Secure?, —By: R. Manoj, Assistant Editor, 'InfoSecurity' magazine. http://www.fanaticmedia.com/infosecurity/archive/Jan%2009/Mobile%20Banking.htm (last visited Feb. 27, 2009).
(2) Mobile Security: A Busy, Buggy Week, Security flaws hit Android, RIM, and MobileMe users, but fixes are available, Amber Bouman, Infoworld, Feb 17, 2009 12:21 pm, http://www.pcworld.com/article/159665/article.html?tk=nl_dnxnws
(3) Mobile Banking: Is this Trend Secure?, —By: R. Manoj, Assistant Editor, 'InfoSecurity' magazine. http://www.fanaticmedia.com/infosecurity/archive/Jan%2009/Mobile%20Banking.htm (last visited Feb. 27, 2009).

...Website examples *(continued from p. 28)*

University of Wisconsin Credit Union
<uwcu.org> and <blog.uwcu.org>

Madison, Wisconsin-based UW Credit Union, a long-time top innovator in Web-based delivery, has the 17th result for "iphone + credit union" search done on Feb 15. This time the link leads to the CU's great blog, *The SourceCode*, which is primarily an online banking educational source.

The topnotch search result from a simple blog entry demonstrates the SEO value of blogging and of featuring a hot, new technology.