Mobile Banking: *Opportunities and Risks*

LORMAN®

Published on www.lorman.com - November 2017

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 120 live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 1,500 courses available
- ☑ **Videos -** More than 1300 available
- ☑ **Slide Decks -** More than 2300 available
- ☑ White Papers
- ☑ Reports
- ☑ Articles
- ☑ ... and much more!

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: www.lorman.com/pass/?s=special20

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

Banking in the Internet era requires an attention to the sensitivity of client data, proper protocol for protecting client information and a thorough understanding of legal issues inherent in the use of mobile banking applications. Banks like Chase have resorted to the use of mobile banking applications due to the increased opportunities that they present for building a client base. Customers love the ease, convenience and freedom to use a mobile banking application at any time. They can easily transfer funds amongst accounts without having to travel to a bank's branch.

When a bank decides to use electronic systems to create a mobile banking application, it must be aware of privacy concerns, technology patents and risks presented by this technology. This paper addresses the concerns that bankers and attorneys charged with representing the best interests of financial institutions should keep in mind when dealing with issues relating to mobile banking applications.

The Use of Additional Due Diligence

The Federal Financial Institutions Examination Council IT Handbook and Retail Payment Systems Booklet are great resources for a professional banker or banking attorney to consider in learning more about issues presented by mobile banking technology and applications. The overarching premise of these documents is that banking professionals must perform additional due diligence if customers utilize these applications for storage of a User ID or password, storage of personal information, transfer of funds or transmission of other information.

Banking attorneys should be aware that traditional regulatory compliance laws still apply in the modern era of banking technology. Some of these laws may not yet be interpreted to outright state the inclusion of mobile banking technology, but attorneys should assume these laws are directly applicable to such technology. The Gramm-Leach-Bliley Act and Regulation P are some of the most important laws that banking attorneys must keep in mind when assessing whether a banking mobile application complies with federal law. These laws require that a bank uses effective risk management practices to protect the transmission of sensitive information through mobile banking apps.

The Federal Deposit Insurance Corporation also maintains suggestions that attorneys should consider in assessing the safety of mobile banking systems. Attorneys should ensure that the mobile banking system uses encrypted technology to secure the information of customers. An SMS system would be an example of an unsafe and risky channel to use for mobile banking systems. The information transmitted on SMS systems cannot be encrypted, and this would entail placing sensitive client information at risk for being released to identity thieves. In the banking industry, only 44 percent of all mobile banking apps were considered safe for the public's use. Over 50 percent of the mobile banking apps required a warning or failed the safety test. See www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html. These statistics indicate that many financial institutions may be at risk or liable for the release of sensitive customer data in the event of a major security threat or hacking incident.

Ways to Provide Mobile Banking Options to Customers

Many financial institutions are now making mobile banking apps easily accessible for customers. Customers may be able to download an app from iTunes or other popular app stores. In just a minute or two, the app is downloaded on one's smartphone. Mobile apps are usually free of cost. There are also no fees for using mobile banking apps.

Capabilities of Mobile Banking Applications

Financial institutions can now offer a variety of mobile banking options for customers. Customers now have the opportunity to check the status of their accounts at all times. They can log into their checking and savings accounts to check balances. Financial institutions also give clients the opportunity to view check transaction history for a period of up to 60 or more days.

Transfers Available

One of the main advantages of mobile banking applications is that customers can transfer funds. Customers can schedule transfers of funds amongst their various bank accounts. They can also view scheduled transfers or transfer activity.

Stop Payment

Banking mobile apps also give customers the chance to stop payment. A customer may discover that he or she written a bad check or needs to stop payment for other purposes. Customers can stop payment on a check if they do not wish to expend funds on a purchase or even are experiencing identity theft. Mobile banking apps make stopping checks much easier and more efficient.

Schedule Payments

Mobile banking apps also give customers an opportunity to organize their finances and schedule payments. Scheduling a payment can assist a customer who may have a busy schedule or have a problem with forgetting to make payments. Customers may want to set up an automatic payment system to make their monthly payments. A mobile banking app also allows customers to view scheduled and processed payments.

IT Infrastructure Required for Support of Mobile Banking Applications

Mobile banking apps can be used on a smartphone or personal digital assistant (PDA) device. Financial institutions now must adhere to significant regulations in creating IT infrastructure for mobile banking apps. The IT infrastructure is the foundation of a mobile app and provides the secure structure that customers need. Many IT infrastructure systems are very old and still prone to damage. Banks now need to process millions of transactions a day, and many banks are not prepared to meet this challenge with the IT infrastructure that they currently use.

U.S. and international banks are now spending millions of dollars to upgrade the IT infrastructure used for mobile banking apps. In 2014, banks invested 25 percent additional funds in IT solutions in comparison with previous years. A modern IT infrastructure system can increase the processing time for transactions.

Banks that seek to learn more about modern infrastructure regulations should visit www.fbiic.gov. One can learn more about the Financial and Banking Information Infrastructure Committee (FBIIC) on this website. The Financial and Banking Information Infrastructure Committee (FBIIC) is currently charged with the task of improving communication amongst financial institutions and regulators. The website also contains policies in regards to national security of consumer information that is held on mobile banking systems.

The FBIIC also conducts risk assessments to determine the safety of cyber-based components in the finance sector. The FBIIC also seeks to provide continuous verification of the safety measures used for mobile banking applications. Major players in the finance sector have a responsibility to provide security and resilience measures in the mobile banking applications that they use.

Financial institutions must ensure that they have compliance measures in place to fulfill the requirements of the National Infrastructure Protection Plan. Leaders in the banking sector have a duty under the law to work with the FBIIC to coordinate the maintenance of an effective infrastructure. See www.dhs.gov/xlibrary/assets/nipp_snapshot_banking.pdf.

The U.S. Department of Homeland Security is also charged with the task of protecting the financial sector and its infrastructure. The U.S. Department of Homeland Security aims to prevent power outages and cyber-attacks that can negatively impact mobile banking technologies. See www.dhs.gov/financial-services-sector.

Security Concerns of Using Mobile Banking Applications

Financial institutions must be aware of the cyber threats that can impact the safety of mobile banking applications. IT professionals and other security professionals need to implement authentication systems that can protect customers at all times. Financial institutions must also be mindful of the great threat that digital terrorists and criminals can pose to the security of sensitive customer data. Without cyber-security measures in place, a financial institution may not be able to deal with cyber-attacks. Financial institutions can resort to encryption methods, continuous threat assessments and countermeasures to prevent cyber-attacks.

Compliance officers may also want to consult with the Federal Financial Institutions Examination Council (FFIEC) Guidance on Authentication. Compliance officers should seek to use a multi-layered approach to authentication and security too. Banks may need to require that customers register a smartphone with an online account and also enter a password for accessing bank accounts through a mobile device. Every year, compliance officers should also perform a risk assessment of compliance measures used to protect client information.

Every financial institution must seriously regard the authentication process used to protect information in mobile devices. Authentication ensures that the correct owner of an account is logging into his or her accounts. Strong authentication controls prevent criminals from gaining access to accounts.

Required Disclosures

Financial institutions are required to send certain updates and disclosures to consumers. They should be aware of Regulation E, which allows financial institutions to provide mobile disclosures. A financial institution also may have an obligation to provide certain disclosures on the front page of a mobile banking app. These disclosures include that one is an Equal Housing Lender and is FDIC Insured.

Banks should be prepared to adhere to the Fair and Accurate Credit Transactions Act (FACTA). Under FACTA, a financial institution must make disclosures and alert consumers about the threat of identity theft. Ideally, a financial institution should make consumers aware of various risks associated with using a mobile banking app. A bank may want to warn consumers that a password should remain protected and not be shared with others. Banks may also want to encourage consumers to only use secure and private networks.

Monitoring Malware

Financial institutions can also monitor malware and the development of potential viruses. IT departments may be able to assess cyber-threats before they make their way into a bank's system. A financial institution can also assess Internet gateways and network servers to prevent cyber-attacks. By continuously monitoring trends involving cyber-threats, financial institutions can be prepared to quickly respond to these threats or resort to counter-attacks.

Security Measures for Mobile Operating Systems (OS)

Several security solutions now exist for smartphones that utilize the OS system. Banks can use permission lists for the installation of mobile banking applications. They can also provide application certificates for each user that downloads a mobile banking app.

It is also important that banks are prepared to deal with cyber-threats presented by Wi-Fi connections. When a user logs onto a Wi-Fi hot spot, cyber criminals may attempt to hack into the user's bank account. Malware may enter the user's smartphone or other mobile device and seek to gather information in it. Users should also be aware of the risks of logging into their bank accounts on a public Wi-Fi connection. If possible, they should try to log onto a bank account using a secure or private Wi-Fi connection.

The Use of Remote Deposit Capture

Many mobile banking applications entail the use of Remote Deposit Capture. Remote Deposit Capture (RDC) allows a user to deposit items directly from a mobile phone. A user may deposit his or her check into an account with this function. Remote Deposit Capture entails taking a photo of the front and back of a check. After the check is authenticated, it may then be deposited into the consumer's account. Compliance officers need to carefully assess the software used to facilitate Remote Deposit Capture. They should also communicate with a vendor about the manner in which check images will be processed. The main concern that a financial institution needs to address in regards to RDC is that criminals may be more prone to engage in money laundering. Banks can eliminate some of the risks of money laundering by ensuring that the only checks accepted are U.S.-based. Banks can also impose limits on the number of remote deposits that may be utilized. Some banks have also placed a limit on the amount of cash that can be deposited through RDC.

Compliance officers should also monitor suspicious activity in regards to RDC. If a compliance officer notices that numerous deposits are being made every day, he or she may be alerted to possible money laundering activity. Financial institution attorneys may even want to preserve the right to eliminate a customer's ability to use RDC if they abuse the privilege. See www.aba.com/Products/bankcompliance/Documents/SeptOct12CoverStory.pdf.

Assessing the Background of Vendors

If a financial institution works with vendors to produce certain technologies, such as RDC, the financial institution should take care to research the background of the vendor. A financial institution should perform its due diligence and make sure that the vendor is licensed. Compliance officers may want to make sure that other clients have had a positive experience in working with a vendor. Compliance officers should also ensure that a vendor has no criminal past or history of violating financial regulations.

Financial institution attorneys may want to carefully select other compliance officers that work for the bank. Banking attorneys may want to ensure that a compliance vendor offers controls that can be applied to a mobile banking app. It may also be important that a compliance vendor can perform audits and ensure that mobile technology meets compliance regulations.

Compliance officers should take care to understand all of the entities that are players in assessing security of mobile banking devices. In addition to government organizations, other entities like the CTIA-Wireless Association may be patrolling cyber security of mobile banking apps. CTIA is responsible for issuing guidelines that can provide excellent advice to compliance lawyers in the position of assessing a financial institution's cyber-security. These guidelines can help compliance officers thoroughly understand industry standards that must be met to authenticate a user's identity. The guidelines can also help compliance officers understand the disclosures that a bank must make. Banks may be under an obligation to disclose liability limits for fraudulent transactions. If a consumer is a victim of identity theft, a bank may only be required to compensate the consumer up to a certain amount. There may also be guidelines that require app users to provide their consent. Also, banks must provide disclosures for any fees that a user may incur for using mobile banking services. See www.aba.com/Products/bankcompliance/Documents/SeptOct12CoverStory.pdf.

Privacy Risks to Consider

Every financial institution must have a plan in place to prevent identity theft. When a financial institution creates a mobile banking application, identity theft can be a main concern. Every banking attorney must undertake the process of implementing a written identity theft prevention program. The Federal Deposit Insurance Corporation (FDIC) maintains specific rules about the topics that must be addressed by an identity theft prevention program. One of the relevant laws that every banking attorney should know is the Fair and Accurate Credit Transactions Act of 2003. See www.fdic.gov/news/news/financial/2007/fil07100.html.

Legal Issues Associated with Use of Mobile Banking Applications

Compliance officers and banking attorneys also must make sure that a mobile banking app is in accordance with the Safeguards Rule. The Safeguards Rule requires that a financial institution make efforts to ensure that customer information remains secure. Any financial institution that provides products or services related to finance must comply with the Safeguards Rule. Entities like payday lenders, mortgage lenders and online tax preparers also need to pay special attention to the Safeguards Rule. Any type of financial entity that uses a mobile banking app should assess its compliance with the Safeguards Rule.

The Federal Trade Commission (FTC) puts forth several ways in which compliance officers can ensure that a financial institution complies with the Safeguards Rule. First, a financial institution should designate an employee who coordinates the information security program of the bank. The employee should also identify the role of a customer's information in the use of services or products created by the financial institution. An employee should regularly assess the effectiveness of compliance programs in protecting the customer's information. The safeguards program should be regularly monitored and tested by the compliance officer. Financial institutions should also be mindful of the protections in place for consumer information when employees have access to it. If an employee has access to a customer's information through his or her own laptop computer or other personal device, a financial institution may need to provide safeguards.

Hiring New Employees and the Applicability of the Safeguards Rule

To provide for greater security of consumer information, financial institutions must be very careful in hiring employees who may have access to this information. The Safeguards Rule requires that financial institutions perform a background check of every employee who may have access to sensitive client information. If a background check indicates that an employee has a history of identity theft or violating the privacy of others, then this is an indication that the employee will likely not be responsible in handling sensitive consumer information. Financial institutions should take care to contact references associated with the individual.

New employees should also receive thorough training in a company's privacy policies if they will be exposed to data transmitted through mobile banking applications. The financial institution should try to limit an employee's access to consumer data to the extent that it is necessary for one's job. Banks can also provide strong protection for client information by requiring that employees use a case-sensitive password to login to information systems. Banks should ensure that strong passwords are used and updated on a regular basis. These passwords should contain upper- and lower-case letters as well as numbers, symbols and odd letter combinations.

All employees should also be aware of the privacy policies of a financial institution. Banks should regularly provide seminars and documents that clearly address their privacy policies. Also, financial institutions should take care to send these disclosures to employees who may work from virtual locations. Every employee should understand the seriousness of protecting consumer information that is transmitted through mobile banking applications.

If an employee is terminated from his or her position, compliance officers or HR professionals should immediately cut off the employee's access to any client files. Banks need to be aware that an employee may still know certain passwords that can provide the employee with access to customer information. It is important that a bank change passwords or otherwise prevent an employee from accessing banking systems.

Ultimately, banking attorneys need to stay updated on the ever-changing laws and regulations that impact the development of mobile banking applications. Maintaining client privacy is one of the main goals of implementing compliance measures in regards to mobile banking applications. Every banking attorney and financial professional needs to understand the new risks posed by the use of mobile banking apps to protect customers from identity theft and cyber-attacks.