APPENDIX E: WIRELESS BANKING

OVERVIEW

Wireless banking occurs when a customer accesses a financial institution's networks through cellular phones, pagers, and personal digital assistants (or similar devices) via telecommunication companies' wireless networks. While wireless services can extend the reach and enhance the convenience of an institution's banking products and services, wireless communications currently have certain limitations that tend to increase the risks associated with this delivery channel.

RISK IMPLICATIONS

Wireless banking services can significantly increase a financial institution's level of transaction/operations and strategic risks.

Transaction/Operations risk – Wireless services create a heightened level of potential operations risk due to limitations in wireless technology. Security solutions that work in wired networks must be modified for application in a wireless environment. The transfer of information from a wired to a wireless environment can create additional risks to the integrity and confidentiality of the information exchanged.

Strategic risk – Financial institutions considering wireless services should carefully evaluate the significant strategic risks posed by this service delivery channel. Standards for wireless communication are still evolving, creating considerable uncertainty regarding the scalability of existing wireless products. Financial institutions should exercise extra diligence in preparing and evaluating the cost-effectiveness of investments in wireless technology or in decisions committing the institution to a particular wireless solution, vendor or third-party service provider.

RISK MANAGEMENT

Risk management of wireless-based technology solutions, although similar to other electronic delivery channels, may involve unique challenges created by the current state of wireless services and wireless devices. Some of these special considerations are discussed below.

MESSAGE ENCRYPTION

Encryption of wireless banking activities is essential because wireless communications can be recorded and replayed to obtain information. Encryption of wireless communications can occur in the banking application, as part of the data transmission process, or both.

Transactions encrypted in the banking application (e.g., bank-developed for a PDA) remain encrypted until decrypted at the institution. This level of encryption is unaffected by the data transmission encryption process. However, banking application-level encryption typically requires customers to load the banking application and its encryption/decryption protocols on their wireless device. Since not all wireless devices provide application-loading capabilities, requiring application level encryption may limit the number of customers who can use wireless services.

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system. A key risk-management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a secure socket layer (SSL) encryption standard and vice versa. Wireless network security reviews should focus on how institutions establish, maintain, and test the security of systems throughout the transmission process, from the wireless device to the institutions' systems and back again. For example, a known wireless security vulnerability exists when the Wireless Application Protocol (WAP) transmission encryption process is used. WAP transmissions deliver content to the wireless gateway-server where the data is decrypted from WAP encryption and re-encrypted for Internet delivery. This is often called the "gap-in-WAP" (e.g., wireless transport layer security (TLS) to Internet-based TLS). This brief instant of decryption increases risk and becomes an important control point, as the transaction may be viewable in plain text (unless encryption also occurred in the application layer). The WAP Forum, a group that oversees WAP protocols and standards, is discussing ways to reduce or eliminate the gap-in-WAP security risk.

Institutions must ensure effective controls are in place to reduce security vulnerabilities and protect data being transmitted and stored. Under the GLBA guidelines, institutions considering implementing wireless services are required to ensure that their information security program adequately safeguards customer information.

PASSWORD SECURITY

Wireless banking increases the potential for unauthorized use due to the limited availability of authentication controls on wireless devices and higher likelihood that the device may be lost or stolen. Authentication solutions for wireless devices are currently limited to username and password combinations that may be entered and stored in clear text view (i.e., not viewed as asterisks "****"). This creates the risk that authentication credentials can be easily observed or recalled from a device's stored memory for unauthorized use.

Cellular phones also have more challenging methods to enter alphanumeric passwords. Customers need to depress telephone keys multiple times to have the right character displayed. This process is complicated if a phone does asterisk password entries, as the user may not be certain that the correct password is entered. This challenge may result in

users selecting passwords and personal identification numbers that are simple to enter and easy to guess.

STANDARDS AND INTEROPERABILITY

The wireless device manufacturers and content and application providers are working on common standards so that device and operating systems function seamlessly. Standards can play an integral role in providing a uniform entry point to legacy transaction systems. A standard interface would allow institutions to add and configure interfaces, such as wireless delivery, without having to modify or re-write core systems. Interoperability is a critical component of mobile wireless because there are multiple device formats and communication standards that can vary the users' experience.

WIRELESS VENDORS

Institutions typically rely on third-party providers to develop and deliver wireless banking applications. Reliance on third parties is often necessary to gain wireless expertise and to keep up with technology advancements and evolving standards. Third-party providers of wireless banking applications include existing Internet banking application providers and as well as new service providers specializing in wireless communications. These companies facilitate the transmission of data from the wireless device to the Internet banking application. Outsourced services may also include managing product and service delivery to multiple types of devices using multiple communication standards. Institutions that rely on service providers to provide wireless delivery systems should ensure that they employ effective risk management practices.

PRODUCT AND SERVICE AVAILABILITY

Wireless communication "dead zones" – geographic locations where users cannot access wireless systems – expose institutions and service providers to reliability and availability problems in some parts of the world. For some areas, the communications dead zones may make wireless banking an unreliable delivery system. Consequently, some customers may view the institution as responsible for unreliable wireless banking services provided by third parties. A financial institution's role in delivering wireless banking includes developing ways to receive and process wireless device requests. Institutions may find it beneficial to inform wireless banking customers that they may encounter telecommunication difficulties that will not allow them to use the wireless banking products and services.

DISCLOSURE AND MESSAGE LIMITATIONS

The screen size of wireless devices and slow communication speeds may limit a financial institution's ability to deliver meaningful disclosures to customers. However, use of a wireless delivery system does not absolve a financial institution from disclosure requirements. Moreover, limitations on the ability of wireless devices to store documents

may affect the institution's consumer compliance disclosure obligations.[18] Additionally, any institution that opts to rely upon voice recognition technology as a means to overcome the difficulty of entering data through small wireless devices should be aware of the uncertain status of voice recognition under the E-SIGN Act.[19]

Wireless banking may expose institutions to liability under the Electronic Fund Transfer Act (Regulation E) for unauthorized activities if devices are lost or stolen. The risk exposure is a function of the products, services, and capabilities the institution provides through wireless devices to its customers. For example, the loss of a wireless device with a stored access code for conducting electronic fund transfers would be similar to losing an ATM or debit card with a personal identification number written on it. However, the risk to the institution may be greater depending on the types of wireless banking services offered (e.g., bill pay, person-to-person payments) and on the authentication process used to access wireless banking services.

[18] Under the Electronic Signatures in Global and National Commerce Act, Pub. L. 106–229, (E-SIGN Act), to obtain effective consumer consent to receiving electronic disclosures, financial institutions must among other things inform consumers of the hardware and software requirements for retention of electronic records that will be provided as disclosures. 15 USC 7001(c)(1)(B). This requirement should be carefully considered by institutions whose customers wish to use wireless devices with limited storage as their primary access device.

[19] The Act specifically provides that an oral communication will not qualify as an "electronic record." 15 USC 7001(c)(6). The treatment of voice recognition technology under this provision is uncertain.