"Your Key to a Wealth of Information"
SNODGRASS
Certified Public Accountants and Consultants

VOL. 3 | AUGUST 27, 2014

INFORMATION TECHNOLOGY UPDATE

Mobile Banking – Proceed with Caution

I'm sure you've noticed how dependent people have become on their mobile devices. It seems everywhere we look people are interacting with some personal computing device, whether it's at work, at play, walking down the street, or—heaven forbid—while driving. It's hard to deny from a strategic standpoint that these technologies present companies with a real opportunity to retain customers or attract new ones. Most financial institutions seem to be offering some degree of mobile banking services or are at least considering adopting mobile banking applications in their suite of services. However, there are a number of risks that should be considered before jumping into the mobile banking marketplace.

A security assessment firm, IOActive, recently studied the security features of 40 mobile banking apps for iOS, including the apps used by some of the world's leading financial institutions. IOActive reported that 40 percent of the apps tested had compromised transport mechanisms that leave app users susceptible to man-in-the-middle attacks. IOActive also found that 90 percent of the apps tested contained non-SSL links, which allow attackers to intercept traffic to the app and inject arbitrary code, such as creating fake login prompts to steal usernames and passwords. Finally, 50 percent of the apps tested were vulnerable to JavaScript injections, making the apps prone to cross-site scripting attacks.

Additionally, mobile devices have given rise to new social engineering threats such as SMiShing. SMiShing, or Short Message Service (SMS) phishing, involves sending bogus text messages that direct recipients to visit a website or call a phone number to entice them to provide sensitive information such as credit card details or passwords.

In looking at the regulatory landscape governing mobile banking, one thing becomes apparent: mobile banking has regulators' attention. In fact, over a dozen laws and regulations have implications for mobile banking depending on the specific banking services being offered, including:

- Gramm-Leach-Bliley Act (GLBA)
- USA Patriot Act
- Bank Secrecy Act/Anti-Money Laundering (BSA/AML)
- Electronic Fund Transfer Act (Reg E)
- Electronic Signatures in Global and National Commerce (E-Sign Act)
- Fair and Accurate Credit Transactions Act (FACTA) - Red Flags Rule
- REGs B, C, E, M, Z, CC, and DD

The FFIEC *IT Examinations Handbook* Appendix E – Mobile Banking, outlines the strategic and operations/transaction risks to consider in offering mobile banking services:

- Encryption – Should consider the security of systems throughout the transmission process.
- Password Security – Authentication credentials may be viewable when being entered or stored in clear text.

This update is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this update, the information contained herein should not be acted upon without professional advice related to your specific situation.

- Standards and Interoperability – There are many device formats and communication standards that must be considered to achieve the desired end-user experience.
- Vendors – Institutions that rely on vendors for these services should ensure that proper vendor due-diligence processes are in place.
- Product and Services Availability – Geographic communication dead zones should be considered when offering these services and may warrant performance disclaimers to customers.
- Disclosure and Message Limitations – Use of wireless delivery requires thought to ensure meaningful disclosures are delivered to customers. There are also liability considerations if inadequate security controls or lost or stolen devices result in unauthorized access to customer information or financial transaction capabilities.

When looking at mobile banking solutions, financial institutions should ensure the service provider has considered these risk areas within the design of their applications, and these areas should be addressed within the financial institutions' policies and procedures to ensure the risks are sufficiently mitigated.

CTIA-The Wireless Association®, in association with the leading U.S. wireless carriers, has developed best practices and guidelines to establish an environment where mobile financial services transactions are authorized, secure, and compliant with applicable laws and industry guidelines, and to protect user privacy and financial data. These best practices include the following areas for consideration:

1. Authentication – Use methods consistent with industry best practices to authenticate user identity that may include multi-factor authentication methods.
2. Alerts and Transaction Records – Provide users the ability to receive banking and payment alerts and notices in accordance with their preferences. Provide systems that allow users to access transaction records and other information about their accounts.
3. Limiting Liability for Unauthorized Transactions – Should disclose all material information regarding the liability, if any, that the user may bear for unauthorized transactions or fraudulent use.
4. Disclosure of Terms; Disclaimers – These should be disclosed in a clear and conspicuous manner to users prior to their use of the service.
5. Consent to Enrollment – Obtain affirmative consent from the user prior to enrollment.
6. Compliance with Laws and Regulations – Provide the product in accordance with all applicable local, state, and federal laws, payment network rules, and mobile industry best practice guidelines.
7. Security of Data Transmissions – Utilize industry best practices when providing security of data during transmission.
8. Security on the Mobile Device or in Storage – Use industry best practices to protect against unauthorized access to data on a mobile device. Such protections may include PIN protection, remote device disabling or wiping, and encryption of sensitive information on the device.
9. Access Controls and Security of Sensitive Information – Offer access control options and tools that enable users to protect their data. Educate users on the importance of protecting their personal information and the use of application security features and capabilities.
10. Fraud and Identity Theft Protection – Offer tools to protect users' information, funds, credit, and identities, such as proactive user identification, detection and response to transaction/use patterns, practices or specific activities, customer ability to place limitation on spending, etc.
11. Collection, Use, and Disclosure of Information – Provide clear disclosures about access, collection, use, storage, and disclosure of personally identifiable information. In the event of a security breach, respond in accordance with relevant breach notification laws.

12. Dispute Resolution Processes and Customer Service – Develop reasonable dispute resolution processes for handling disputed payments and transactions and provide customer service via an appropriate method and at commercially reasonable times.

A well-designed mobile banking solution that considers the risks of the services being offered and addresses the regulatory requirements and security best practices should help financial institutions navigate safely into the mobile banking marketplace.

Questions?

If you wish to discuss any of the above items, please contact Jeremy Burris or Rob Haller at (724) 934-0344, or email at jburris@srsnodgrass.com or rhaller@srsnodgrass.com.

This update is intended to provide timely, accurate, and authoritative information on the subject matter herein. Due to the general nature of this update, the information contained herein should not be acted upon without professional advice related to your specific situation.