GreenPoint>
Legal

IS YOUR MOBILE DEVICE SAFE FOR FINANCIAL TRANSACTIONS? CAN YOU BANK ON IT?

With worldwide mobile banking usage expected to exceed 1 billion users by 2017, mobile users seek assurances that their handheld banking transactions will be secure, and financial institutions need to keep abreast of emerging mobile banking regulations. This article will examine mobile banking from both perspectives.

Security—a Main Concern of Mobile Users

According to a study by Javelin Strategy and Research, the main concern of customers who performed bank transactions via their mobile devices was the safety of their confidential information. Today's mobile banking technology allows the same level of security as provided by a desktop computer; however, the fear of losing a cellphone loaded with passwords for bank accounts has some mobile users skittish about going mobile for bank transactions.

Three Main Application Platforms

Mobile banking applications are based on three different technologies: SMS, mobile web (Internet browser-based) or proprietary client apps. A charitable donation can be made by simply sending a text message, a check can be deposited using Remote Deposit Capture (RDC), which scans checks and then transmits the image to your bank, and Person-to-Person (P2P) payments that allow you to transfer a sum directly to another person without writing a check.

Is one technology more secure than another? In theory, the bank's own proprietary application is more secure because it is synched with the bank's security algorithms. It is, of course, important that the customer download the app from the bank's website or from another trusted, known third-party source.

Old Rules for New Technology

For the most part, the same regulations that have applied to online banking also apply to mobile banking. The element that requires special attention for the mobile app provider is the authentication protocols necessary for validating a customer who is communicating with his or her account via a mobile device.

The Federal Financial Institutions Examination Council (FFIEC) offers security guidelines for e-banking in general. The guidelines do not specifically deal with mobile banking but do suggest a "layered approach" for security: Initially customers must register their device with an existing account, then create a unique password and enter the password each time the account is accessed. Some banks require periodic change of the password and personal security questions such as "what was your first car?" In the future, biometrics may be used to authenticate the user.

A risk assessment is required for every new technology being introduced—including for mobile banking—and the assessment must be renewed each year.

As with the innovation of online banking, customer education is key to keeping mobile banking safe and secure.

PETER K. OVERZAT, ESQ • 212.913.0500 x557 • 917.807.1321 • PETER.OVERZAT@GREENPOINTGLOBAL.COM
DAVID KINNEAR • 212.913.0500 x565 • 917.886.3222 • DAVID.KINNEAR@GREENPOINTGLOBAL.COM • WWW.GREENPOINTLEGAL.COM
A Division of GreenPoint Global