Mobile banking increases efficiency, but how secure is it?

More treasury professionals want to conduct business when they’re on the go, and Mobile SinglePoint® from U.S. Bank lets them do it securely.

The Mobile SinglePoint app and the mobile-optimized website enable treasury managers, and other authorized employees, to use mobile devices to execute a variety of banking functions, such as:

- View balances and transaction details
- Approve Automated Clearing House (ACH), wire and book transfer transactions
- Transfer funds
- Deposit checks remotely
- Decision Positive Pay exceptions

Mobile banking can make companies more efficient and improve cash management. A good example is a company whose drivers or service technicians collect checks from customers in the field. With a mobile remote deposit capture service, these employees can use a mobile device to deposit checks immediately after receipt, instead of returning to the office to drop off checks for deposit. This saves them time and allows them to focus on their core duties. It can also eliminate deposit delays and improve the company’s access to funds.

A consistent security framework

Mobile SinglePoint operates under the same security standards and policies as the SinglePoint online banking solution. “We’ve leveraged the security infrastructure in place on the web to enhance the security of mobile transactions,” says Randy Lade, group product manager at U.S. Bank.

Before a client can use one of the U.S. Bank mobile banking solutions, a decision-maker or system administrator within their organization must authorize access.
Continued from page 7...

From there, all the approval processes and security infrastructure incorporated within the SinglePoint web solution are employed within the mobile offering. To start, before they can log in, employees must enter a user identification number and password.

**Hard or soft token authentication**

Users then complete a secondary authentication. This can be done through a hard token (or fob) that regularly generates random numbers. To gain access, users must enter the number displayed on their tokens at the time they’re logging into the system.

Mobile SinglePoint also offers users the option of soft token authentication in the form of a text message sent to their phones. Again, they must enter the code provided by the text before they can access the system. This alternative often appeals to users who don’t want to carry hard tokens, or whose organizations have policies against hard tokens being taken off premises, Lade says.

**Additional controls**

Once on the system, a user’s ability to access different functions is controlled by an administrator. These granular entitlements ensure that employee access to Mobile SinglePoint is limited to those functions required to perform their jobs.

In addition, any approval requirements in place for transactions conducted online are incorporated within Mobile SinglePoint. For example, employees who initiate repetitive payments through Mobile SinglePoint are required to obtain the same secondary approvals as configured under their SinglePoint web customer ID.

**Mobile RDC safeguards**

Similar safeguards are deployed with the U.S. Bank mobile remote deposit capture (RDC) solution, which enables users to deposit checks remotely using a supported mobile device. “Mobile is an extension of our On-Site Electronic Deposit platform,” notes Stephanie Schmitt, group product manager at U.S. Bank.

A system administrator must grant permission before a user can use their mobile device to deposit checks to U.S. Bank. Users must also complete the dual authentication process. Companies can customize the service to require secondary review and approval of check deposits for added security and oversight.

U.S. Bank, along with many other financial institutions, also leverages tools to detect suspicious activity including duplicate deposits in the event that a client also makes a deposit through a traditional banking channel such as a branch. Clients are required to “frank” or mark checks, which is another way to identify an item as deposited. However, it’s not a foolproof process, Schmitt says. Additional safeguards are necessary to protect U.S. Bank and its clients. Banks have introduced monitoring processes to detect suspicious activity.

Continued on page 9...
Who owns the device?

When implementing mobile treasury solutions, one question that often arises is the benefit and security of requiring employees to access treasury apps only from corporate-owned devices — versus allowing employees to use their own personal devices. Policy on this can vary from one company to another.

“In either case, none of the security requirements or processes need to change,” Lade explains. On both corporate-owned and personal devices, a company can require its system administrator to allow employees access to the system, and require users to complete the dual authentication process.

Innate security features

In addition to the security features provided through Mobile SinglePoint, mobile devices have some inherent security features. Each mobile phone, of course, is assigned a unique phone number. In addition, many devices require users to enter credentials, such as passwords, before they can use them. Some require biometric authentication such as a thumbprint.

U.S. Bank is currently exploring the addition of biometric authentication security to its Mobile SinglePoint offerings. Indeed, U.S. Bank continues to evaluate its mobile strategy and security offerings.

“We want to ensure we’ve leveraging innovations that will meet our clients’ evolving needs,” Lade says.