



FINANCIAL LITERACY TIP OF THE WEEK

FOR IMMEDIATE RELEASE

April 29, 2013

APRIL IS FINANCIAL LITERACY MONTH

MOBILE AND ONLINE BANKING: THE PROS, CONS, AND THE FUTURE

(Boise) – Idaho Governor C.L. "Butch" Otter has declared April as Financial Literacy Month. As part of an ongoing effort to provide Idahoans with cutting edge information, tips and updates on financial services, the Department of Finance discusses the pros, cons, and the future of mobile banking.

As more Americans migrate toward mobile and online banking, consumers need to know not only what services and cyber protections are being offered by their financial institutions, but also the steps they must take to protect their private information in cyberspace. "Mobile banking is not a dream; it is a reality," Department of Finance Director Gavin Gee said. "The current and upcoming technology to provide banking at our fingertips is growing by leaps and bounds; it is powerful. Consumer education and savvy about its benefits and pitfalls are key components for those who want to safely manage their mobile banking services."

The Federal Reserve's 2013 *Consumers and Mobile Financial Services* study found that 87 percent of the U.S. adult population has a mobile phone, and 28 percent of those have used mobile banking. Mobile banking includes bill payment, person-to-person payments, alerts and notices, and remote deposit capture. Many of these types of technologies are widely available at financial institutions as their clientele gravitates toward easy and accessible banking services. Financial institutions also are aware that they need to ensure they are addressing all risks associated with online and mobile banking and implementing the necessary controls, where appropriate.

PROS OF MOBILE BANKING

The upside of mobile banking is simple: Consumers have quick and efficient access to viewing and managing their money anytime and anywhere their mobile device has service. Today, consumers have the ability to receive alerts, transfer funds, deposit checks and pay bills via their smartphone devices. Having access to account information at their fingertips can save time and avoid late fees and overdrafts.

However, consumers need to remember that nothing comes without the cost of due diligence. Consumers have an obligation to check with their financial institution to determine the terms, conditions and potential costs associated with mobile services before they sign up.

CONS OF MOBILE BANKING

The #1 concern voiced by consumers regarding mobile banking is the potential lack of security and protection in cyberspace. Before using mobile banking, consumers should determine their comfort level with using this technology to perform financial transactions. Consumers are obligated to become a partner with their financial institution in detecting and preventing fraud.

Reports about mobile banking have a similar tone. That industry is leading the way to make certain security is in place for mobile banking. Financial institutions are aware that fraudsters already know how to hit mobile technology. Solutions and strategies are being discussed and implemented to address mobile fraud as the trend toward mobile banking unfolds.

NEW TECHNOLOGY

In the future financial institutions will offer mobile “off and on switches” for debit cards so that a consumer can deactivate their card if it is lost or stolen or if they suspect fraud.

A new application called “Picture Play” already is available at some financial institutions. This service enables customers to pay a bill by taking a picture of it on their mobile device.

Some institutions are developing voice recognition software that will enable customers to handle banking transactions by speaking commands into their mobile device.

The “mobile wallet” is being rolled out – a device that will analyze the mobile user’s spending habits and guide them in paying bills and making purchases most efficiently. The mobile wallet will help the consumer make purchases with the “best” credit card, and help manage their budget based on their spending habits.

To help ensure consumer safety, the **Federal Deposit Insurance Corporation** offers these tips at its Web site <http://www.fdic.gov/consumers/consumer/news/cnwin1213/mobilebanking.html> :

- **Be proactive in securing the mobile device itself.** Depending on what security options are available on your device, create a “strong” password and periodically change it.
- **Be careful about where and how you conduct transactions.** Don't use an unsecured Wi-Fi network, such as those found at coffee shops, because fraud artists might be able to access the information you are transmitting or viewing.
- **Take additional precautions in case your device is lost or stolen.** Check with your wireless provider in advance to find out about features that enable you to remotely erase content or turn off access to your device or account if you lose your phone.
- **Research any application (“app”) before downloading it.** Many apps that appear official are actually fraudulent apps designed to trick users.
- **Be on guard against unsolicited e-mails or text messages appearing to link to a financial institution's Web site.** Those could be “phishing” messages designed to lead you to a fake Web site controlled by thieves.

If you are a victim of fraud and suspect your personal information has been compromised, follow the Federal Trade Commission’s ID theft guidelines for fraud victims. For more advice, contact the FTC’s ID Theft Consumer Response Center at 1-877-ID THEFT (1-877-438-4338) or www.ftc.gov/idtheft.

For more information on mobile and online banking visit the Idaho Department of Finance’s website. The Department’s Web site at <http://finance.Idaho.gov> provides links to the FDIC’s and the FTC’s websites, both of which contain further information on mobile banking.

###

Department of Finance Press Releases and other information can be found on the Internet via the Worldwide Web at <http://finance.idaho.gov> or may be obtained by contacting the Department at (208) 332-8000 or Idaho toll-free at 1-888-346-3378.