Financial Security

Tips On Protecting Your Financial Information

(NAPSA)—By partnering with financial institutions—such as banks, credit unions and credit card companies—and taking a few easy steps, you can help to protect yourself from fraud.

Guard personal and financial information: Take extra measures to protect your Social Security number. That means not sharing it unnecessarily, not using it as your password and not carrying information with you that contains the number. You should also avoid sharing personal details that are often used to access financial accounts—such as your birth date, home address and mother's maiden name.

Monitor your accounts: Remember to review account activity regularly, especially during the holiday shopping season, when you may be spending more than usual. By monitoring your accounts online—at your bank and credit card websites—and setting up account alerts that can be sent via e-mail or mobile device, you can spot suspicious activity early. Notify your financial institution immediately of any unknown or suspicious transactions.

Go paperless: Fraudulent activity can result from mail and garbage theft, so consider switching to online statements. Online bank statements look and function just like paper statements—you can use them for record keeping and taxes.

When possible, replace paper invoices, statements and checks with electronic versions if your employer, bank, utility provider or merchant offers them. If you have to keep some paper statements, be sure to shred them before discarding, and always shred documents that contain personally identifiable information, such as Social Security numbers.

Avoid sharing personal details that are often used to access financial accounts—such as your birth date, home address and mother's maiden name.

Recognize fraudulent communications: Fraudsters use a variety of methods to obtain your information: Phishing is when fraudsters send an e-mail that appears to come from a reputable company with links to spoof websites requesting your personal and account information. Vishing is a phishing attempt made through a telephone call or voice message, and smishing is a phishing attempt sent via SMS (Short Message Service) or text message to a mobile phone or device.

Never share personal or financial information through unfamiliar e-mails, websites, social media networks, text messages or phone calls.

Ensure you're protected: Check with your financial institution to learn if you're covered if funds are removed from your account without your permission. For example, Wells Fargo's Online Security Guarantee provides added protection against unauthorized access to your accounts.

Visit Wells Fargo's Fraud Information Center at www.wellsfargo.com/privacy_security/fraud for more tips on how to protect yourself.