NORTHERN TRUST

# FRAUD PREVENTION TIPS FOR CONSUMERS

April 2018

Never give anyone your PIN or password, no matter who they claim to be.

## PROTECT YOURSELF FROM SOCIAL ENGINEERS & FRAUD

The threat of Social Engineering remains one of the top security risks in the modern world. Social Engineers typically use any means available to get the information they want — information that can then be used to perpetrate Identity Theft, commit fraud, or be exploited for other illicit purposes.

### WHAT IS SOCIAL ENGINEERING?

Social Engineering is a term used to describe a collection of techniques used to manipulate people into performing harmful actions or divulging confidential information. Social Engineers often portray themselves as people in need of your help or people in authority to gain access to information they are not authorized to receive.

### WHAT CAN I DO TO PROTECT MYSELF AND MY FAMILY?

There are many types of Social Engineering scams which can be used individually or in various combinations. Both individuals and businesses are targets of Social Engineers, and scams often target older adults. Educating yourself and your family members about common social engineering threats is one of the best ways to avoid this type of fraud. In addition to knowing what's out there, there are a few key things you can do to help protect yourself from these dangers, as described below.

- **Protect your account numbers and passwords.** Do not share your passwords and/or account numbers with others. Use care when writing down passwords, ATM pins, and other sensitive financial information to ensure that information is protected. If you keep a list of User IDs and passwords on your personal computer or mobile device, make sure they are protected by a unique password or passphrase and avoid calling the file "passwords". If possible, encrypt saved documents that contain User IDs and password information or use "Password Vaults".
- **Know that wiring money is like sending cash.** Social Engineers are nothing more than con artists, and the most common scams are simply bogus attempts to obtain money. Tricking victims into wiring money is a favorite con of fraudsters because it is nearly impossible to reverse the transaction or

### REAL WORLD EXAMPLE

In a scam currently circulating in London, victims are telephoned by a suspect who alleges to be someone of authority (e.g., from the police, bank, or Serious Fraud Office). The suspect tells the victim there is a problem with their bank account (for example, that the account has been compromised) and that their bank card must be collected. Victims are asked to reveal their bank details, namely the PIN. The scam is completed when a courier or taxi driver is sent to collect the victim's card. The card is delivered to the criminal, who then withdraws funds from the account, completing the fraud and leaving the victim with an empty account.

Always remember — don't give anyone your PIN or password, no matter who they claim to be!

trace the money. Never wire money to strangers or to sellers who insist on wire transfers for payment. Don't even wire money to someone claiming to be a relative or friend experiencing an emergency until you verify the authenticity of the family member and the emergency. ■

- **Be wary of in-person, mail, phone or Internet solicitations that you did not initiate.** Scams of this nature may involve notices that you've won money ("you've won a raffle / lottery / sweepstakes prize"), Debt Relief, offers of lower credit card interest rates, home repairs, mortgage assistance, fake charities, and many more. Before responding to any offers of this nature, discuss with a trusted personal friend or family member. If it sounds too good to be true, it probably is. ■
- **Contact your financial institution if something looks suspicious.** It's common for fraudsters to approach consumers pretending to be their bank or credit card company. Before providing any information, contact the institution directly through your regular channels (i.e., in-person visit, phone call to the number on your card or statement) to confirm the request is legitimate. ■
- **Dispose of all personal documents by shredding.** Shred receipts, insurance forms, credit applications, physician statements, checks, bank statements, expired credit or debit cards, and all other personal documents before disposing of them for maximum protection against dumpster diving criminals.
- **Lock your financial documents.** All financial documents, personal records, lists of passwords, and other sensitive personal information should be kept in a secured area away from visitors, roommates, or workers who may come into your home. ■
- **Don't be afraid to ask!** Before sharing information with your physician's office, your child's schools, or other businesses, ask why they need it. Find out how they protect your information and be specific about whether or not they are authorized to share your information and with whom. ■

- **Consider a locked mailbox.** For incoming mail, consider a locked mailbox to protect against thieves who may be targeting personal information or checks. For sensitive outbound mail, consider taking to a post office or post office collection or wall box. ■
- **Be smart on-line.** If using Social Networking sites, be sure to understand and properly set your privacy controls. Avoid oversharing — information about vacations and business trips may alert thieves to an empty home, while answering "quizzes" and "getting to know you" type activities may provide scammers with all the information they need to answer your Security Challenge Questions and reset your passwords. Never post your full name, your social security number, your phone number, or your exact address on-line. Educate your children about appropriate on-line behavior and be clear about what information should not be shared on-line.