Title: Information Security: Preventing Identity Theft

Revision Log:

<table>
<thead>
<tr>
<th>Who:</th>
<th>When:</th>
<th>Why:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overview:

- **Time:** 30 minute course
- **Recommended for:** Any branch employee who handles identifying or sensitive information
- **Updated date:** December 2011

Objectives:

Following the course, participants should be able to:

- Define identity theft and describe how it occurs
- Identify common identity theft scams
- Describe how criminals use the identifying information
- Identify account activities that serve as red flags of fraud
- Describe the S.E.C.U.R.E. method and how it helps to prevent information loss

Description: This course is designed for all personnel of financial institutions with access to customer information, especially new accounts personnel, tellers, customer service representatives, and loan officers. Upon completion of this course, learners will be able to define identity theft, describe the type of information criminals seek, identify scams and explain how the S.E.C.U.R.E. method prevents information loss.

Do not distribute.
## Content: Introduction

What You Need to Know About the Risks.

### Risk 1
**Who is responsible for preventing identity theft?**
All employees have a legal responsibility and obligation to protect customer information. By recognizing your role in securing customer information, your actions will become routine, which may lessen instances of identity and information theft.

### Risk 2
**What are the steps to help minimize the risk?**
Employees must be proactive and understand the necessary steps to secure information from ending up in the wrong hands. These steps help ensure:
- all documents are properly destroyed or stored in accordance with financial institution policy,
- customer conversations are private or written,
- customer information on computer screens is minimized, and
- additional security steps are taken when computers are unattended

### Risk 3
**How do thieves steal information?**
Equip yourself with an understanding of how thieves may attempt to obtain information and maintain vigilance to prevent inadvertent disclosure of information. Be prepared to recognize and then notify those designated within the institution to address issues such as “dumpster diving,” “shoulder surfing,” or “phishing”.

### Notes:

---

*Do not distribute.*
### Content: Introduction

Stop identity thieves from stealing more than just your identity!

Criminals can ruin lives with the damage they do when using someone else’s identity. You are entrusted by your customers with very personal information and it is your duty to protect that information.

Get the scoop on what identity theft is, the types of information criminals want, the crimes they can commit with that information and how you can stop them in their tracks.

This course contains important information about how you can protect yourself, your financial institution and your customers from identity thieves.

**NOTE:** Your financial institution may use one or more terms to reference the people serviced; but, for simplicity, this course will use "customers" to represent the individuals your financial institution services.

<table>
<thead>
<tr>
<th>Media Info:</th>
</tr>
</thead>
<tbody>
<tr>
<td>93946683</td>
</tr>
<tr>
<td>Display note on post-it note graphic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notes:</th>
</tr>
</thead>
</table>
**Content: ID Theft Basics**

Who are identity thieves?

Click and drag each image that you think represents a typical identity thief to the police station. Click "Submit Answer" when you are finished.

Feedback:

**If all images were selected:** That's right! Any one of these people could be an identity thief. You cannot tell by a person's appearance that he or she is a criminal, but you **can** recognize suspicious behavior when you see it. You are responsible for the protection of identifying information, so remain vigilant. All it takes is a brief lapse in judgment or a moment of carelessness for a customer’s identity to be stolen.

**If anything but all images were selected:** Actually, any one of these people could be an identity thief. You cannot tell by a person's appearance that he or she is a criminal, but you **can** recognize suspicious behavior when you see it. You are responsible for the protection of identifying information, so remain vigilant. All it takes is a brief lapse in judgment or a moment of carelessness for a customer’s identity to be stolen.

**Notes:**

Do not distribute.
### ID Theft Basics

**What is Identity Theft?**

Identity theft is “a crime of deception involving the unauthorized use of another individual's confidential identifying information.”

According to the Federal Trade Commission, as many as 9 million Americans have their identities stolen each year. Financial institutions must be diligent in the fight against identity theft.
## Content: ID Theft Basics

### Why Do Identity Thieves Target Banks?

Banks collect an abundance of sensitive information about their customers and consumers, especially the kind of information identity thieves value:

- Social Security Numbers
- Account numbers
- Customers’ names
- Addresses
- Balances

The right information is like an identity thief’s **key to the vault**, enabling him/her to:

- Open accounts in your customers’ names and conduct fraudulent transactions
- Hijack an existing account and liquidate the funds before your customer has time to realize what’s happened

---

**Media Info:**

Building - 94321774

---

**Notes:**
How are Victims Impacted by Identity Theft?

You, as the financial institution representative, your institution and your customers will be impacted if identity theft occurs. Below is a list of ways identity theft impacts its victims. Indicate how the impact of identity theft is experienced by each of these potential victims by clicking the corresponding cell in the chart.

Click "Submit Answer" when you are finished.

<table>
<thead>
<tr>
<th>Type of Impact</th>
<th>You</th>
<th>Your Institution</th>
<th>Your Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal penalties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loss of sense of security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negative publicity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Job loss</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Feedback

Correct selections are highlighted.

**Legal penalties for both you and your institution:** Safeguarding personal identifying information is not just a matter of good service – it’s a legal requirement through the Gramm-Leach-Bliley Act and FACT Act.

**Financial loss for you, your institution and your customer:** You may lose your job, your institution may have to pay financial penalties and your customers may have their entire savings wiped out.

**Negative publicity for your institution:** People need to trust their institution and won’t want to entrust their money to your institution if word spreads that it was careless with protected personal identifying information.

Notes:

Do not distribute.
## ID Theft Basics

### What Types of Information Do Identity Thieves Want?

Identify thieves typically go after two types of information:

<table>
<thead>
<tr>
<th>Personal identifying information</th>
<th>Security information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique documentation needed to open an account</td>
<td>Information to access accounts and make transactions</td>
</tr>
<tr>
<td>• Legal Name</td>
<td>• PIN</td>
</tr>
<tr>
<td>• Street Address</td>
<td>• Username/password</td>
</tr>
<tr>
<td>• Date of Birth</td>
<td>• Account number</td>
</tr>
<tr>
<td>• Identification Number</td>
<td>• Backup security information (mother’s maiden name, town where you were born, first pet’s name, etc.)</td>
</tr>
</tbody>
</table>

How can thieves use this information?

- With these four items, a thief could open a checking account, obtain a line of credit in someone else’s name, and conduct fraudulent transactions. After conducting these illegal activities, the identity thief moves on and leaves behind chaos for the customer.

How can thieves use this information?

- In combination with personal identifying information, a thief could access an already-existing account and remove all funds, perhaps even overdrawning the account. An identity thief could also max out home equity lines of credit before a customer ever knows what is happening.
Criminal Schemes to Steal Identities

Quite often, news stories about identity theft describe advancing numbers of computer-savvy criminals employing high-tech means to steal unsuspecting victims’ personal information via the web.

However, identity thieves may also still operate through “traditional methods” such as rummaging through trash containing sensitive documents or conning someone into providing information.

Criminal schemes can be grouped into three categories:

- Blatant Behaviors – those you can see if you pay attention
- Trust Trampling – when a friend is not a friend
- High-Tech Hijinks – invisible invasions through technology

The next few screens provide insight into the various schemes within these categories.
# Information Security: Preventing Identity Theft

**Date:** 1/5/2012

### Content: Schemes

<table>
<thead>
<tr>
<th>Blatant Behavior: Common Scams in Plain Sight</th>
</tr>
</thead>
<tbody>
<tr>
<td>The average frontline employee may not be able to stop the identity thief who, armed with a laptop and internet connection, worms his/her way into a financial institution's network to access your customers' information.</td>
</tr>
<tr>
<td>Financial institution staff, however, can make a substantial difference by keeping their eyes open for the following scams that can occur in your branch right in full view.</td>
</tr>
</tbody>
</table>

**How do they do it?** Click on each scam for a description.

- **Dumpster Diving** – One of the oldest tricks in the book. The thief rummages through the trash cans in the lobby or the dumpsters behind the institution or branch office, looking for account statements, receipts, credit reports, computer disks, tapes – anything containing personal information that might allow a criminal to assume your customers' identities and commit fraud.

- **Desk/Countertop Skimming** – Identity theft in financial institutions can occur when criminals find sensitive customer documentation on top of file cabinets, on computer screens, or in unlocked cabinets.

- **Shoulder Surfing** – Strictly speaking, a “shoulder surfer” is somebody who hangs around an ATM vestibule, a store counter, or near the drive thru, hoping to sneak a peek at somebody’s PIN number or hear confidential personal information. For the same reason, staff should also keep an eye out for anybody lingering around computer terminals, work-stations, teller lines, or lobby kiosks.

- **Theft** – While certainly not the most creative of methods, it is just as dangerous as any other. While the thief will certainly take advantage of the forgetful customer who leaves the odd deposit or withdrawal slip lying in the lobby, he/she is especially interested in documents, computer disks, tapes, or CDs that you or your customers leave unattended on your desks or workstations.

- **Vendor Access/Theft** – Financial institutions have different vendors throughout the day that have potential access to customer information. Computer tech support, janitors, vending machine stock people, and others may have the chance to steal information if it is readily available.

---

**Notes:** Italicized text appears when link is clicked.
Humans are social creatures and the desire to have trusting relationships is strong. Unfortunately, criminals can take advantage of that desire. **Social Networking** and **Social Engineering** are the two methods identity thieves use to gain trust - and then they use that trust to gain information.

**Social Networking**

Sites such as Facebook, Twitter, and MySpace allow individuals to stay connected and share information with “friends” all over the world. As more individuals join social networking sites, **criminals are using these sites to obtain information to commit crimes including identity theft.**

Studies show that **individuals who have used social networking sites for at least five years may be twice as likely to be victims of identity theft.**

**Remember:**

- Always follow your financial institution’s policies concerning the acceptable use of institution resources and internet access.
- Use a unique username and password for your social networking account. Do not use the username and password that you use for your financial institution’s systems, internet banking or other financial websites.

Click each circle to learn how criminals use social networking and what you can do to prevent it.

[Sample layout for this screen (helps depict the “networking” idea):]
Trust Trampling

Humans are social creatures and the desire to have trusting relationships is strong. Unfortunately, criminals can take advantage of that desire. Social Networking and Social Engineering are the two methods identity thieves use to gain trust and then use that trust to gain information.

Social Networking

Sites such as Facebook, Twitter, and MySpace allow individuals to stay connected and share information with “friends” all over the world. As more individuals join social networking sites, criminals are using these sites to obtain information to commit crimes including identity theft.

Studies show that individuals who have used social networking sites for at least five years may be twice as likely to be victims of identity theft.

Remember:
- Always follow your financial institution’s policies concerning the acceptable use of institution resources and internet access.
- Use a unique username and password for your social networking account. Do not use the username and password that you use for your financial institution’s systems, internet banking or other financial websites.

Click on each circle to learn how criminals use social networking and what you can do to prevent it.
END OF SAMPLE