ID Theft & Account Fraud: Prevention & Cleanup

Seminar Lesson Plan and Class Activities

Lesson purpose:

To provide participants with an awareness of identity theft and account fraud, teach them how to protect their information and prevent ID theft, and provide them with the knowledge and tools they would need to clean up and recover from the damage if they did become fraud victims.

Lesson objectives:

By the end of the lesson, participants will understand:

- the potential damage caused by ID theft and account fraud;
- how ID theft and account fraud happen;
- how to protect their personal data and avoid becoming victims;
- how to recognize when fraud has occurred;
- what their rights are regarding responsibility for fraudulent debts and other fraudulent activity;
- what steps to take if they are, or believe them may become, a victim of identity theft; and
- what resources are available to help consumers and victims.

Lesson duration:

2½ hours (including a 10-minute break; not including 15-minute optional interactive quiz)

Materials:

For instructor:

- *ID Theft & Account Fraud: Prevention & Cleanup* brochure
- Lesson plan (pages 3-14)
- Activities and worksheets (including answer keys) (pages 15-29)
    - ID Theft Prevention Checklist (page 15)
    - *Test Your Knowledge About ID Theft & Account Fraud* quiz and answer key (pages 16-26)
    - *Savvy Consumer* quiz and answer key (pages 27-28)
- Sample letters (pages 29-32)
- Training evaluation form (page 33)
- ID Theft & Account Fraud Leader's Guide
- Visual teaching aid (PowerPoint presentation with instructor's notes)

Instructor will also need:

- A computer and projector for the PowerPoint presentation (*Note:* The PowerPoint slides also can be printed on transparency sheets for use on an overhead projector); and
- An easel and pad, or a whiteboard, and markers.

For participants:

- *ID Theft & Account Fraud: Prevention & Cleanup* brochure
- Worksheets and activities:
    - ID Theft Prevention Checklist (1 page)
    - *Test Your Knowledge About ID Theft & Account Fraud* quiz (2 pages)
    - *Savvy Consumer* quiz (1 page)
    - Sample letters (4 pages)
- Training evaluation form (1 page)
- OPTIONAL: Printout of the PowerPoint presentation

Lesson Outline

- Welcome and training overview (5 minutes)
- How ID theft and account fraud happen (25 min)
- The effects of ID theft and account fraud (10 min)
- Identity theft prevention (includes *ID Theft Prevention Checklist*) (25 min)
- *Activity:* Test Your Knowledge About ID Theft & Account Fraud quiz (20 min)
    - Break (10 min)
- ID theft cleanup (25 min)
- *Activity:* Savvy Consumer quiz (10 min)
- Identity theft resources (5 min)
- Questions and answers (10 min)
- Wrap-up and evaluation (5 min)

- *Activity (OPTIONAL):* Identity Theft Interactive Quiz (downloadable) (15 min)

  The ID Theft Quiz game is an educational tool that can be used to complement and reinforce the ideas and concepts discussed in the ID Theft & Account Fraud training module. To use the game, download the instructions (PDF) and a PowerPoint presentation containing the game slides at www.consumer-action.org/outreach/articles/id_theft_quiz/.

Rev. 3/14

Instructor's Notes:

This training module consists of a brochure (*ID Theft & Account Fraud: Prevention & Cleanup*); a leader's guide written in question-and-answer format; a lesson plan that includes class activities; and a PowerPoint presentation. It was created by the national non-profit organization Consumer Action to be used nationwide by non-profit organizations providing personal finance, consumer and housing education in their communities.

Before conducting the training, familiarize yourself with the brochure, the leader's guide, the lesson plan (including activities), and the PowerPoint visual teaching aid.

The PowerPoint presentation contains notes for each slide (appearing below the slide when in Normal view or Notes Page view). These notes offer detailed information about the items appearing on the slide. Additional key points are inserted into the lesson plan when needed. The lesson plan includes indicators so you will know which slide corresponds to each part of the lesson, and when to move to the next one.

Why Adults Learn, a PowerPoint training for educators, provides tips for teaching adults and diverse audiences—it will be helpful to you even if you have taught similar courses before. The slide deck is available at the Consumer Action website (www.consumer-action.org/outreach/articles/why_adults_learn/).

Welcome and training overview (5 minutes)

➡**SLIDE #1** (onscreen as participants arrive; direct participants who arrive early to begin reading the brochure; review slide notes during pre-training preparation)

Welcome participants. Introduce yourself and present the purpose of the training and the agenda.

➡**SLIDE #2**

Go over items on slide and in the slide notes.

If you have a small group, you can ask individuals to introduce themselves (or, if time permits, ask them to pair off with someone seated near them and then introduce each other to the group) and tell you what they hope to get out of the training. In a larger group, invite volunteers to share their expectations. On your whiteboard or easel pad, jot down some of the specific things participants mention. You can come back to this at the end of the training to make sure you've covered these points. (This activity is designed to serve as a brief icebreaker. It will also give you an idea what participants' expectations and needs are.)

Review the contents of participants' packets. Ask the class to take a look inside their packets and make sure they have all the materials needed.

How ID theft and account fraud happen (25 min)

Learning objective: *Understand how ID theft and account fraud happen*

Discuss what identity theft and account fraud are and why it's important to be aware of these types of crimes. Identify the different types of ID theft that can occur. (See Leader's Guide "About Identity Theft" section.)

➡SLIDE #3

Questions to generate discussion:

- Do you think that identity theft is increasing or decreasing? *(It has been increasing.)*
- Is there a typical victim of identity theft? *(No. Victims now include virtually everyone, from babies to senior citizents—even the deceased.)*

Share a statistic:

- Identity theft is the #1 subject that the Federal Trade Commission (FTC) receives complaints about each year. The most common type of identity theft involves stealing victims' identities in order to apply for federal benefits. Also common are cases in which thieves use credit card data, unwittingly supplied by consumers, to make unauthorized purchases.

➡SLIDE #4

Questions to generate discussion:

- What is identity theft? What is account fraud? *(Chances are that some of the participants in the class have firsthand experience with ID theft, or know of someone who is or has been a victim.)*
- Why do you think it's important to learn about identity theft and account fraud? *(Allow a moment or two for participants to respond. You can jot down responses on your easel pad or whiteboard. Then reveal the next slide.)*

Key points about ID theft and account fraud:

- There are many different ways that ID thieves use the personal information they steal.
- The types of identity theft are changing to include things like child, medical, criminal or "synthetic" ID theft.
- While traditional ("true name") identity theft has gotten easier to detect or thwart through tools like credit monitoring, fraud alerts and credit freezes, other types of ID theft have gotten harder to detect.

➡SLIDE #5

Key points about medical ID theft:

- Medical ID theft occurs when someone obtains medical care or prescription drugs under your name, or files false insurance claims on your policy.

- Medical ID theft can result in more than just financial costs—your health and you're your life could be at risk because of inaccurate medical records generated from the theft.
- Suspicious medical bills or denied coverage by your health insurance company because you've already reached your benefits limit are signs of potential medical identity theft.
- You have the right to review your medical records and request that mistakes are corrected.
- You can reduce the chances of medical ID theft by being careful with your medical insurance card, shredding medical documents you no longer need and keeping your medical information private.

➡SLIDE #6

Key points about criminal ID theft:

- Criminal ID theft occurs when an impostor commits a crime or misdemeanor and gives another person's name and personal information to a law enforcement officer or investigator.
- Because criminal ID theft doesn't show up in your credit report, it can be difficult to detect before it becomes a serious problem (for example, when you are notified there is a warrant for your arrest or you are denied employment).

➡SLIDE #7

Key points about child ID theft:

- Stealing a child's identity can be particularly attractive to a thief because the crime can go undetected for far longer since children are not actively applying for credit, insurance, employment, etc. (scenarios where they might be alerted to a negative credit report).
- Bills, pre-approved credit offers in the child's name are signs of potential identity theft, as are collection calls, notifications from the IRS that the child's Social Security number has already been used on another return, or denial of public benefits because the child is already listed on another households account.
- You have the right to opt out of sharing certain information with your child's school.
- Child welfare agencies are required to check the credit reports of foster children age 16 and older.

➡SLIDE #8

Key points about theft of a deceased person's identity:

- Thieves sometimes target the deceased because it can be a long time before creditors learn of the death and close accounts or the credit bureaus deactivate the deceased consumer's files.
- Calls from a creditor or collection agency about an account opened or used in the deceased's name after death is a sign of possible identity theft.
- You can decrease the chances of this type of ID theft by limiting the details you provide about the deceased in the obituary and by taking the initiative to notify creditors,

insurance companies, credit bureaus, financial institutions, government agencies, etc. about the death as soon as possible.

➡SLIDE #9

Present the many methods thieves and fraudsters employ to obtain the personal data they use to commit their crimes. (See Leader's Guide "About Identity Theft" section.)

Questions to generate discussion:

- What are some ways you can think of that thieves might use to steal someone's identity? *(List responses on your easel pad or whiteboard.)*
- What do you think "familiar fraud" is? Can you give an example? *("Familiar fraud" is when the victim knows the ID thief—for example, a roommate who steals your account information from a billing statement in your room, or a relative who steals your Social Security number.)*

Key points about how thieves get their victims' information:

- "Familiar fraud" is what ID theft is called when the thief is a person known to the victim.
- Thieves can steal personally identifiable information in a variety of ways, including finding or stealing your wallet, phone or computer, taking the mail out of your box or filing a change of address, rummaging through your trash (called "dumpster diving"), watching as you punch in your password or PIN or listening as you say your credit card number, sending "phishing" messages,buying customer information from a dishonest employee, intercepting your information as you shop online at unencrypted sites or use social media, and accessing your phone rcords.
- Phishing messages often purport to be from agencies and companies other than your bank.
- You can reduce the chances of a thief getting your private information by taking precautions such as using a strong passcode for computers and mobile devices, shredding papers before you discard them, guarding your belongings, shielding the keypad as you enter your passcode, not responding to any message that you are not entirely confident is legitimate, etc.

Share a statistic:

- Consumers between the ages of 25-34 are most likely to be victims of "familiar fraud," which is fraud perpetrated by people known to the victim, such as a relative or roommate. *Source: IdentityTheftAssistance.org*

➡SLIDE #10

Key points about "insider" ID theft:

- ID theft often is an "inside job," perpetrated by an employee, employer, family member, friend or acquaintance.
- If the ID thief is a family member or friend, you must decide whether or not to involve police.

➡**SLIDE #11**

Questions to generate discussion:

- How many large companies (such as a wireless service provider or bank), institutions (such as a school or hospital) and government agencies (such as the IRS or the Social Security Administration) can you think of that have your personal information (SSN, birth date, credit card numbers, etc.) in their databases?
- Have you ever received notification that your information was part of a data breach? What was the outcome? Did you feel that the company/institution/agency did enough to protect your information, notify you promptly and/or resolve the situation to your satisfaction?

Key points about data breaches:

- There are many ways a security breach can occur—all of which are out of your control.
- A majority of states have laws requiring that individuals be notified when a breach compromises their personal information. In some cases, even if your state does not have a security breach notification law, you may be entitled to notification under federal law.
- Data breach victims are at higher risk to become fraud victims, so pay attention to any notifications you receive and take advantage of any offer from the company for free credit monitoring.

The effects of ID theft and account fraud (10 min)

Learning objective: *Understand the effects of ID theft and account fraud, including financial and other (non-financial) costs*

Present the potential costs of identity theft and the toll it can take on victims. Include a brief explanation of victims' right to not be held accountabe for fraudulent debt.

➡**SLIDE #12**

Questions to generate discussion:

- What are the costs to victims of identity theft and account fraud? **Hint:** Don't think only in terms of financial costs. (*Encourage learners to think of more than just the cost in dollars—the cost in hours (to do all the legwork to clear your name), the cost in lost opportunities (for example, if your damaged credit causes you to be rejected for a rental home, a loan or a job), the emotional toll, etc.)*
- How/why does it pay to put some effort into preventing identity theft?

Key points about the costs/toll of ID theft:

- The effects of ID theft can be financial, emotional and legal. Victims can lose hours of their time trying to clean up the mess. They may even pay the fraudulent debts just to end the ordeal. ID theft can take an emotional toll (stress resulting from collection calls, rejected applications, etc.). It can result in missed opportunities, higher costs for credit, and affect job performance. You could even be mistakenly arrested.

- You are not held liable for fraudulent debt. However, there may still be some out-of-pocket expenses.

Share a statistic:

- The average cost to an ID theft victim rose slightly to $365 in 2012, up from $354 in 2011. *Source: Javelin Strategy & Research*

Identity theft prevention (25 min)

Learning objective: *Understand how to avoid becoming a victim*

Explore the various ways that consumers can reduce their chances of becoming victims of identity theft and account fraud. Stress the importance of monitoring credit reports and specialty consumer reports and taking steps to keep personal information private. (See Leader's Guide "Preventing Identity Theft" section.)

➡SLIDE #13

Questions to generate discussion:

- What are some ways you could make it more difficult for identity thieves and scammers to get your information? *(List responses on your easel pad or whiteboard.)*
- How many of you already do one or more of these things?

Key points about ID theft prevention:

- Protect your information: Track your mail, shred documents, monitor your account transaction statements, keep your PINs and passwords secret, notify agencies (IRS, DMV, SSA) if you have reason to be concerned, place a deceased alert when a loved one passes.
- Password protect your cell phone and your phone service account records.
- Monitoring your credit reports regularly is one of the best ways to catch identity theft early.
- Monitor specialty consumer reports, as well. You are entitled to a free report every 12 months.

➡SLIDE #14

Key points about medical and prescription reports:

- Specialty reports don't exist for everyone, but it's likely there is at least one report on most people.
- The Medical Information Bureau (MIB) compiles reports that insurance companies use to determine someone's health risk level. Not everyone has an MIB file.
- IntelliScript and MedPoint report drug purchase histories.

➡SLIDE #15

Key points about residential tenant reports:

- ID thieves can gain access to your personal information for the sole purpose of using it to rent an apartment or house.
- There are at least four major tenant history report companies (see slide notes for details).
- If you are looking to rent, consider ordering your tenant report(s) before you apply so that you can correct any inaccuracies or be prepared to explain any negative information.

➡SLIDE #16

Key points about check-writing history reports:

- ChexSystems provides information used by banks and credit unions when you try to open an account. They can also use the information to try to collect on unpaid overdrafts and fees.
- Certegy (formerly SCAN) and TeleCheck both track instances of returned checks and checking account fraud for use by retailers and other businesses that accept checks.

➡SLIDE #17

Key points about employment data reports:

- Employment data reports are not the same as employment background check reports.
- The Work Number tracks employment and income history as well as employer-sponsored medical and dental benefits and unemployment claims.
- The Work Number will also help child support workers locate non-custodial parents by providing information on most recent employment. Social service agencies may also use The Work Number to verify eligibility for benefits.

➡SLIDE #18

Key points about insurance claims history reports:

- ID thieves can use your stolen identity to obtain insurance policies or make false insurance claims.
- There are separate reports for auto claims and personal property (homeowners/renters) claims.

➡SLIDE #19

Key points about employment background check reports:

- An employer must ask your permission before requesting a credit or background report on you—your job application may not be considered if you say no.

- If the employer decides not to hire or promote you or fires or reassigns you because of information in your report, you must be given a copy of the report.
- You might not be able to get a free annual copy of your report because some screeners evaluate you but do not maintain a file.
- More decision-makers (employers, lenders, etc.) are running social media background checks or doing their own social media checks on applicants—something you should consider as you decide what to share on social media.

➡SLIDE #20

Key points about utility reports:

- Consumers' telephone and utility account histories are used by service providers to determine whether and how much of a deposit to require on new accounts, and to collect past-due amounts on old accounts.
- If an identity thief has opened and/or abandoned an account in your name, it could appear here.

➡SLIDE #21

Key points about Internet safety:

- The Internet is a valuable tool, but not everybody on the Internet is your friend or has your best interests at heart.
- There are many threats on the Internet, some of which can result in the theft of your identity.
- There are many precautions you can take and tools you can use to protect your information on the Internet.
- Employers *and* ID thieves check social media for information, so it's a good idea to be careful about what you share—in other words, don't reveal too much.
- By law, parents have some control over the online collection of their children's personal information.

➡SLIDE #22

Key points about placing an active duty alert:

- An active duty alert is a special form of protection for members of the military who are away from their regular duty station.
- The alert requires creditors to verify your identity before granting credit in your name.

Question to generate discussion:

- How many of you have learned at least three things you should do differently to protect your private information? *(If you have time, you can ask for volunteers to name something they will now do differently.)*

Ask participants to remove the ID Theft Prevention Checklist from their packets and have them check off the things on the list they have already done. Encourage them to use the list after class as a guide for next steps.

Activity: Test Your Knowledge About ID Theft & Account Fraud quiz (20 min)

Ask participants to take the *Test Your Knowledge About ID Theft & Account Fraud* quiz from their folders.

You can have participants work on the exercise alone or have them break into small groups and work together to answer the questions. (If you are running short on time, you can split the room into two groups and have each group work on one of the two pages, or break it into three groups and assign five questions to each group.) Ask for volunteers to answer questions (if done individually) or rotate among groups for responses, allowing the spokesperson from each group to provide the correct answer along with their reasoning.

Break (10 min)

Announce a 10-minute break. Make yourself available for a few minutes to direct people to the restroom or a place to get drinks and snacks.

ID theft cleanup (25 min)

Learning objective: *Understand what steps to take if you become a victim of ID theft*

Explain how consumers might discover that their identity has been stolen. Go over specific things that consumers can do to discover identity theft early and limit the damage.

➡SLIDE #23

Questions to generate discussion:

- Frequently, victims of ID theft are unaware that their identity has been stolen. How could that be?
- How do you think you could find out if your identity has been stolen? What are some signs that would indicate you might be a victim of identity theft? *(See slide notes for examples.)*

Key points about spotting evidence of identity theft:

- You have to be aware of the signs of identity theft in order to stop it as soon as possible.
- Inmates can be at greater risk, so before leaving prison, they should take steps to find out if they find out if their identities were used while they were incarcerated.

➡SLIDE #24

Discuss what to do if you become a victim of identity theft. Go through the specific steps that victims should take to clear their names and limit the damage. (See Leader's Guide "Advice for Victims" section.)

Questions to generate discussion:

- What are some of the steps you think a victim would need to take to undo the damage done by an identity thief?
- Whom do you think you should notify if you become an ID theft victim?

Key points about ID theft cleanup:

- It's important to file a police report—it will help you deal with creditors, collectors, etc.
- Close the accounts that you know have been tampered with or opened fraudulently.
- By law, companies must give you a copy of the application or other records relating to your identity theft if you submit your request in writing, accompanied by a police report. *(Refer participants to their packets for the "Letter to existing creditors.")*

➡SLIDE #25

Key points about placing a fraud alert:

- A fraud alert can help protect you from identity theft.
- The 90-day initial alert entitles you to one additional free credit report annually; an extended (seven-year) alert allows you to get two additional reports within 12 months.
- You only have to contact one of the three credit reporting agencies; your alert will automatically be sent to the other two.
- It will take longer to open a new credit account if you have a fraud alert on your report, so allow for extra time.
- There is no charge to place a fraud alert on your file.

➡SLIDE #26

Key points about freezing your credit:

- A security freeze makes your credit file off-limits. This usually means a credit request will be denied. It will also lock out insurance companies, landlords, employers who need to do a background check, cell phone companies, utilities, and others.
- You can lift the freeze before someone needs to access your credit report, or you can provide the PIN or password that the credit reporting agency gives you.
- A security freeze will not keep out anyone with whom you already have an account or other business relationship, and it will not prevent fraud involving your existing financial or credit accounts.

➡SLIDE #27

Key points about ID theft services:

- In most cases, a credit report monitoring service that charges a monthly or annual fee is not necessary.

➡**SLIDE #28**

Key points about dealing with collection agencies:

- Never agree to pay for a debt that is the result of identity theft. Tell the collector you are a victim of ID theft and are not responsible for the account.
- Takes detailed notes of all conversations with collectors and creditors, keep all letters you receive regarding the identity theft, and send letters by certified mail, return receipt requested.
- It is important to repair your credit report if there are unauthorized charges or accounts opened in your name.

Note: Contrary to what you might think, a new Social Security number may not be the answer to your problem. It may actually make things worse because you may not have any credit history at all. The Social Security Administration only assigns new numbers in limited cases.

***Activity:* Savvy Consumer quiz (10 min)**

Ask participants to take the *Savvy Consumer* quiz from their folders.

Participants can break into small groups and work together to answer the questions, or can work individually. (If you are running short on time, you can assign just one question to each of five groups.) Ask for volunteers to answer the questions or rotate among the groups for responses, allowing the spokesperson from each group to provide the correct answer along with what the subject did right and wrong and what s/he should do next.

Identity theft interactive quiz (OPTIONAL) (15 min)

The Identity Theft Quiz game is an educational tool that can be used to complement and reinforce the ideas and concepts discussed in the ID Theft & Account Fraud training module. To use the game, download a PDF containing the instructions and rules, and a PowerPoint presentation containing the game slides, at www.consumer-action.org/outreach/articles/id_theft_quiz/.

Identity theft resources (5 min)

Introduce some of the available identity theft resources and how each can help. If you can project your computer screen, visit the sites and show participants where they can go to find valuable information. (See Leader's Guide "Identity Theft Resources" section.)

➡**SLIDES #29, #30, #31**

Questions and answers (10 min)

Preparation: Review the *ID Theft & Account Fraud: Prevention & Cleanup* brochure and the ID Theft & Account Fraud Leader's Guide. The guide is written in Q&A format to help you anticipate frequently asked questions.

Open the floor to questions.

Wrap-up and evaluation (5 min)

➡**SLIDE #32**

Congratulate learners on their participation in the class. Thank them for attending and ask them to fill out the evaluation form and leave it on a table or in a large envelope you provide. If you will be conducting other trainings at a specific future time, announce that now and encourage learners to attend.

ID Theft Prevention Checklist

Put a checkmark in the boxes next to the actions you have already taken to safeguard yourself from identity theft. Use the list as a guide for next steps to protect yourself from fraud, checking off each item as you complete it.

Review credit reports

□ Ordered my credit reports (*www.annualcreditreport.com / 877-322-8228)*

□ Reviewed my credit reports

□ Disputed all questionable and inaccurate information with the credit reporting agency(ies)

□ Placed an active duty alert in my credit files (servicemembers only)

Password all accounts

□ Placed strong passwords on credit card, financial (checking/savings) and phone accounts

□ Asked companies I do business with to not use my mother's maiden name as an identifier

Social Security number

□ Memorized my Social Security number

□ Ordered a new driver's license and/or checks without my Social Security number on them (if necessary)

Computer safety

□ Bookmarked favorite sites (to avoid spoof sites)

□ Password-protected my smartphone/PDA and set it to lock during inactivity

Miscellaneous

□ Switched to a locking mailbox (or requested that landlord install one)

□ Read privacy policies of the companies I do business with; changed my privacy settings/options where necessary

□ Opted out of prescreened credit offers

If you are an identity theft victim:

□ Filed a report with the police department and received a case number

□ Filed reports with other appropriate agencies, such as the U.S. Postal Inspection Service, the Federal Trade Commission, the DMV, the Social Security Administration and my state's attorney general

□ Downloaded and completed a free FTC ID Theft Affidavit (www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf)

□ Put a fraud alert or security freeze on my credit report

Equifax Security Freeze: 800-685-1111; Experian Security Freeze: 888-397-3742; TransUnion Security Freeze: 888-909-8872.

Test Your Knowledge About
ID Theft & Account Fraud

Take this quiz to see how much you know about identity theft and account fraud prevention and cleanup. Check "True" or "False" to answer the following statements.

1. You may not find out that you are a victim of identity theft until you review your credit or specialty consumer reports or a credit card statement and notice charges you didn't make.

❏ True ❏ False

2. Identity theft and account fraud occur when an impostor uses your personal identification information to commit fraud or uses your credit card number to make unauthorized charges.

❏ True ❏ False

3. The National Consumer Telecom & Utilities Exchange is used to determine if you are required to pay a deposit for telecommunication services and the amount of that deposit.

❏ True ❏ False

4. Fraudsters who use your identity for medical care or services can introduce changes to your medical record that can pose a risk to you.

❏ True ❏ False

5 Typically, consumers are not held liable for fraudulent debts.

❏ True ❏ False

6. Under FCRA and FACTA you have a right to free reports from all nationwide specialty agencies every 12 months.

❏ True ❏ False

7. You are entitled to a free copy of the credit report that was used in the decision to deny your credit application.

❏ True ❏ False

8. ChexSystems is a specialty consumer reporting agency that maintains a database of returned checks and instances of checking account fraud. It provides check authorization and verification to member retailers.

❏ True ❏ False

9. An employer must get your permission to conduct a background check on you, but if you are denied employment because of information in a background report, the employer is not required to show you the report or tell you how to get a copy of it.

❏ True ❏ False

10. Phishing is an attempt to "hook" you into revealing your personal and confidential information by sending emails that seem to come from a legitimate business.

❏ True ❏ False

11. To place an "active duty" alert, or to have it removed, servicemembers must call the fraud department of one of the three nationwide consumer reporting companies.

❏ True ❏ False

12. Suspicious accounts or incorrect information appearing in your credit file, calls from collection agencies, bills or account statements not arriving in the mail, and unexplainable denial of credit applications are all signs that you may be a victim of identity theft.

❏ True ❏ False

13. An initial fraud alert is appropriate if your wallet has been stolen or you've been taken in by a "phishing" scam, or if a company that you do business with notifies you that your personal information was compromised due to a security breach.

❏ True ❏ False

14. An extended fraud alert stays on your credit report for five years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an identity theft affidavit.

❏ True ❏ False

15. A credit freeze will prevent ID thieves from opening up new accounts using your personal information because credit issuers will not be able to access your credit file.

❏ True ❏ False

Answer Key for the *Test Your Knowledge About ID Theft & Account Fraud* Quiz

1. You may not find out that you are a victim of identity theft until you review your credit or specialty consumer reports or a credit card statement and notice charges you didn't make.

TRUE: Unfortunately, many consumers learn that their identity has been stolen only after some damage has been done—for example, when collection agencies contact them for overdue debts they never incurred; when they apply for a mortgage or car loan and learn that problems with their credit history are holding up the financing; or when they get something in the mail about an apartment they never rented, a house they never bought or a job they never held.

According to the FTC, the best way to find out sooner rather than later if you are a victim of identity theft is to monitor your accounts and bank statements each month and check your credit reports on a regular basis.

(See www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html*)*

2. Identity theft and account fraud occur when an impostor uses your personal identification information to commit fraud or uses your credit card number to make unauthorized charges.

TRUE: ID theft refers to crimes in which someone uses another individual's personal information, such as name, Social Security number, birth date, mother's maiden name or other identifying information, to commit fraud. In many cases, the thief steals an identity to commit financial fraud, such as borrowing money or making purchases on accounts opened in the victim's name. The thief typically defaults on the payments and leaves the victim to clean up the mess.

According to the FTC, identity theft is inherent in numerous other types of fraud, including mortgage fraud and fraud schemes directed at obtaining government benefits, including disaster relief funds. The IRS's Criminal Investigation Division, for example, has seen an increase in the use of stolen SSNs to file tax returns. In some cases, the thief files a fraudulent return seeking a refund before the taxpayer files. When the real taxpayer files, the IRS may not accept his return because it is considered a duplicate return. Even if the taxpayer ultimately is made whole, the government suffers the loss resulting from paying multiple refunds. Account fraud is another form of fraud—this is the use of someone else's existing accounts, such as credit cards or bank accounts, to make unauthorized purchases or withdrawals.

*(See ID Theft Leader's Guide (*www.managing-money.org/articles/id_theft_account_fraud_leaders_guide1*) and* www.idtheft.gov/reports/StrategicPlan.pdf*)*

3. The National Consumer Telecom & Utilities Exchange is used to determine if you are required to pay a deposit for telecommunication services and the amount of that deposit.

FALSE: According to information on the National Consumer Telecom & Utilities Exchange (NCTUE) website (www.nctue.com), the Exchange is a member-owned database housed and managed by Equifax, one of the three major credit reporting agencies. Membership is available to the nation's leading telecommunication and utility companies.

NCTUE's stated objectives are:

- Early identification of higher-risk accounts for new residential service applicants.
- Locating former customers whose service was terminated with an unpaid balance.
- Identification and implementation of additional uses of the data to benefit members.

Although the NCTUE exchanges information on new connects and defaulted and/or fraudulent accounts among its members, enhances collection and recovery processes by reporting new address and telephone information on defaulted account for 24 months, and provides information used in determining objective methodology for assessing deposits and identification of higher-risk consumer applicants, the company emphasizes that the decision to assess a deposit, and the amount of that deposit, is left up to each individual member.

(See www.nctue.com/nctue*)*

4. Fraudsters who use your identity for medical care or services can introduce changes to your medical record that can pose a risk to you.

TRUE: According to the FTC, recent reports have brought attention to the problem of medical identity theft, a crime in which the victim's identifying information is used to obtain or make false claims for medical care. The FTC warns that every time a thief uses your identity to get care, a record is created with the impostor's medical information that could be mistaken for your medical information—say, a different blood type, an inaccurate history of drug or alcohol abuse, test results that aren't yours, or a diagnosis of an illness, allergy or condition you don't have. Any of these could lead to improper treatment, which, in turn, could lead to injury, illness or worse. Victims of medical identity theft not only may have their health endangered by inaccurate entries in their medical records, they may also have their insurance depleted, become ineligible for health or life insurance, or become disqualified from some jobs. Victims may not even be aware that the fraud has occurred because medical identity theft can be difficult to discover, as few consumers regularly review their medical records. Victims may not realize that they have been victimized until they receive collection notices or they attempt to seek medical care themselves, only to discover that they have reached their medical insurance coverage limits.
(See www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt10.shtm *and* www.idtheft.gov/reports/StrategicPlan.pdf*)*

5. Typically, consumers are not held liable for fraudulent debts.

TRUE: Under various laws, your liability for fraudulent debts caused by identity theft is limited. The FTC offers the following summary:

- **Fraudulent credit card charges:** You cannot be held liable for more than $50 for fraudulent purchases made with your credit card, as long as you let the credit card company know within 60 days of when the credit card statement with the fraudulent charges was sent to you. Some credit card issuers say cardholders who are victims of fraudulent transactions on their accounts have no liability for them at all (referred to as a "zero liability" policy). Note: According to the National Consumer Law Center, consumers are not limited to the 60-day reporting requirement, but the organization noted that the sooner authorized charges are reported, the better it is for the consumer. (See Consumer Facts for Older Americans: www.nclc.org/images/pdf/older_consumers/cf_credit_card_rights.pdf)
- **Lost or stolen ATM/debit card:** If your ATM or debit card is lost or stolen, you may not be held liable for more than $50 for the misuse of your card, as long as you notify the bank or credit union within two business days after you realize the card is missing. If you do not report the loss of your card promptly, your liability may increase.
- **Fraudulent electronic withdrawals:** If fraudulent electronic withdrawals are made from your bank or credit union account, and your ATM or debit card has not been lost or stolen, you are not liable, as long as you notify the bank or credit union in writing of the error within 60 days of the date the bank or credit union account statement with the fraudulent withdrawals was sent to you.
- **Fraudulent checks:** Under most state laws, you are liable for just a limited amount for fraudulent checks issued on your bank or credit union account, as long as you notify the bank or credit union promptly. Contact your state banking or consumer protection agency for more information.
- **Fraudulent new accounts**: Under most state laws, you are not liable for any debt incurred on fraudulent accounts opened in your name and without your permission. Contact your state attorney general's office (www.naag.org/current-attorneys-general.php) for more information.

In cases where a thief commits a more serious crime, such as driving under the influence while using your identity, you may be detained by police and spend time and effort trying to clear up the situation. While, ultimately, you probably will not be held responsible for the crime, the cost in time and money to clear your name can be considerable. For instance, you could be turned down for a job or anything else that requires a background check while false information remains on your record. For more information about criminal identity theft and how to clear your name, visit the Privacy Rights Clearinghouse (www.privacyrights.org).

(See ID Theft Leader's Guide at www.managing-money.org/articles/id_theft_account_fraud_leaders_guide1 *and* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html*)*

6. Under FCRA and FACTA you have a right to free reports from all nationwide specialty agencies every 12 months.

TRUE: Under the FCRA and FACTA, nationwide specialty consumer reporting agencies—those companies that compile reports on consumers for targeted uses, other than credit—must provide a free report to consumers every 12 months, upon the consumer's request.

The Privacy Rights Clearinghouse provides the following examples of the types of reports that specialty consumer reporting agencies compile:

- Medical conditions (for example, the Medical Information Bureau (MIB))
- Residential or tenant history and evictions (for example, the RentBureau)
- Check writing history (for example, ChexSystems)
- Employment background checks (for example, LexisNexis Screening Solutions)
- Homeowner and auto insurance claims (for example, CLUE reports)

(See www.privacyrights.org/fs/fs6b-SpecReports.htm*)*

7. You are entitled to a free copy of the credit report that was used in the decision to deny your credit application.

TRUE: According to the FTC's website, you're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft. Otherwise, a consumer reporting company may charge you up to $11.00 for another copy of your report (beyond your one free annual report) within a 12-month period.

(See www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm*)*

8. ChexSystems is a specialty consumer reporting agency that maintains a database of returned checks and instances of checking account fraud. It provides check authorization and verification to member retailers.

FALSE: There are three major specialty reporting companies that report on checking account history: ChexSystems, Shared Check Authorization Network (SCAN) and TeleCheck.

> **ChexSystems** is a nationwide specialty consumer reporting agency that collects and maintains information from member financial institutions such as banks and credit unions. If a bank closes your checking account because of insufficient funds, for example, it will make a report to ChexSystems that other banks will check when you apply for new accounts.

Shared Check Authorization Network (SCAN) and **TeleCheck** both maintain a database of returned checks and instances of fraud. Both also provide check authorization and verification to member retailers.

(See www.privacyrights.org/fs/fs6b-SpecReports.htm*)*

9. An employer must get your permission to conduct a background check on you, but if you are denied employment because of information in a background report, the employer is not required to show you the report or tell you how to get a copy of it.

FALSE: According to Privacy Rights Clearinghouse, the Federal Credit Reporting Act (FCRA) provides that an employer must give you notice that a background screening may be conducted, and the employer must get your permission to conduct the screening. Notice and permission must be given on a separate document, not buried in an application or another form.

The national standard, set by the FCRA, does not require an employer to tell you the name of the screening company or tell you how to get a copy of your report. But, as is relevant here, the employer must give you a copy of the report if he or she decides not to hire you or denies you a promotion if you are a current employee.

(See www.privacyrights.org/fs/fs6b-SpecReports.htm#8*)*

10. Phishing is an attempt to "hook" you into revealing your personal and confidential information by sending emails that seem to come from a legitimate business.

TRUE: The FTC explains that **"**phishers" send an email or pop-up message that claims to be from a business or organization that you may deal with—for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate" or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site, but it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an email or pop-up message that asks for personal or financial information, do not reply.** And don't click on the link in the message, either. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet

browser—phishers can make links look like they go to one place, but actually send you to a different site.

- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice over Internet Protocol (VoIP) technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.
- **Use antispyware and antivirus software, as well as a firewall, and update them regularly.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Antivirus software and a firewall can protect you from inadvertently accepting such unwanted files. Antivirus software scans incoming communications for troublesome files. Look for antivirus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.
- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a padlock icon in the browser's status bar or a URL that begins "https:" instead of just "http:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges**.** If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- **Be cautious about opening any attachment or downloading any files from emails** you receive regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **Forward spam that is phishing for information** to spam@uce.gov and to the company, bank or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

If you believe you've been scammed, file a complaint with the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html.

(See www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html and www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm*)*

11. To place an "active duty" alert, or to have it removed, servicemembers must call the fraud department of one of the three nationwide consumer reporting companies.

TRUE: The FTC explains that if you are a member of the military and away from your usual duty station, you may place an "active duty" alert on your credit report to help minimize the risk of identity theft while you are deployed. When a business sees the alert on your credit report, it must verify your identity before issuing credit in your name. The business may try to contact you directly, but if you're on deployment, that may be impossible. As a result, the law allows you to use a personal representative to place or remove an alert. Active duty alerts on your report are effective for one year, unless you request that the alert be removed sooner. If your deployment lasts longer, you may place another alert on your report.

To place an active duty alert, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies: Equifax, Experian or TransUnion. The company will require you to provide proof of your identity, which may include your Social Security number, your name, address and other personal information.

- Equifax: 800-525-6285; www.equifax.com
- Experian: 888-EXPERIAN (397-3742); www.experian.com
- TransUnion: 800-680-7289; www.transunion.com

Contact only one of the three companies to place an alert—the company you call is required to contact the other two, which will place an alert on their versions of your report, as well. If your contact information changes before your alert expires, remember to update it.

When you place an active duty alert, your name will be removed from the nationwide consumer reporting companies' marketing lists for prescreened offers of credit and insurance for two years, unless you ask that your name be placed back on the lists before then. Prescreened offers—sometimes called "preapproved" offers—are based on information in your credit report that indicates you meet certain criteria.

(See www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt147.shtm*)*

12. Suspicious accounts or incorrect information appearing in your credit file, calls from collection agencies, bills or account statements not arriving in the mail, and unexplainable denial of credit applications are all signs that you may be a victim of identity theft.

TRUE: Identity theft can go undetected for many months—but there typically are signs of the fraud. Some of these signs include:

- Missing credit card and loan statements, which may indicate that a thief has stolen them from your mailbox or changed your mailing address with your creditors
- Unauthorized purchases on your credit cards.

- Cards and bills for accounts you didn't open, or rejection letters for credit you didn't apply for.
- Calls or letters from collectors about bills you don't recognize.
- Being denied such things as credit, a job, insurance or a home rental for no obvious reason.

Read your account statements promptly and carefully and check your credit report every year—some experts recommend twice a year—even if you haven't seen anything to indicate you are a victim of identity theft. Look for any suspicious activity, such as accounts, loans and inquiries you don't recognize.

(See ID Theft Leader's Guide www.managing-money.org/articles/id_theft_account_fraud_leaders_guide1*)*

13. An initial fraud alert is appropriate if your wallet has been stolen or you've been taken in by a "phishing" scam, or if a company that you do business with notifies you that your personal information was compromised due to a security breach.

TRUE: A fraud alert is a notation on your credit report that requires the three major credit-reporting agencies (Experian, TransUnion and Equifax) to alert you when someone applies for credit in your name. These alerts also are intended to prompt creditors to verify your identity before issuing credit in your name, although they are not compelled by law to do so.

Any consumer can request an "initial" fraud alert, which stays on your report for at least 90 days. This might be appropriate if you have reason to believe you might become a victim of identity theft. For example, you might want to place a fraud alert if you lost your wallet or inadvertently gave information to someone you believe may be a scam artist. You can renew the alert after 90 days.

(See ID Theft Leader's Guide www.managing-money.org/articles/id_theft_account_fraud_leaders_guide1*)*

14. An extended fraud alert stays on your credit report for five years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an identity theft affidavit.

FALSE: According to the FTC there are two types of alert: an initial alert and an extended alert.

An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. An Identity Theft Report such as the ID Theft Complaint available from the FTC website (www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisanidentitytheftreport) should be sufficient to obtain an extended fraud alert. With an extended fraud alert,

potential creditors must actually contact you or meet with you in person before they issue you credit. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for prescreened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: That may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

(See www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisafraudalert*)*

15. A credit freeze will prevent ID thieves from opening up new accounts using your personal information because credit issuers will not be able to access your credit file.

TRUE: A credit security freeze is a much more stringent measure of protection than a fraud alert. Rather than simply alerting you when someone applies for credit in your name, a freeze actually prevents anyone from accessing your credit file until you take steps to give permission by "lifting" the freeze. Companies that can't check your credit report usually won't approve an application for credit, phone service, insurance, housing or employment until you authorize the credit bureau to release your information.
(See Consumer Action's Security Freeze Training Manual (www.consumer-action.org/modules/articles/security_freeze_training_manual_questions_and_answers*) and* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisafraudalert*)*

Savvy Consumer Quiz

Decide whether the consumer in each scenario is savvy (well informed) or not. Be prepared to answer these questions in a class discussion:

- *What did the consumer do right?*
- *What did the consumer do wrong?*
- *What should the consumer do next?*

1. Erica's bank calls. They would like to send her a new credit card and they need to verify some information. Since she was thinking about opening up a new credit card anyway, Erica gives them her Social Security number and birth date.

Erica is: ☐ savvy ☐ not savvy

2. Jason can't find his wallet, which contains nine credit cards, an ATM card and his Social Security card. He contacts the store where he made his last purchase, but it does not have his wallet. He contacts the card companies and his bank to report the loss.

Jason is: ☐ savvy ☐ not savvy

3. Peter and Linda have a joint credit card account. Peter wants to avoid additional interest and late fees by paying the balance in full each month. He notices that the balance is more than usual, but he pays the full amount without questioning the charges because he assumes Linda made them.

Peter is: ☐ savvy ☐ not savvy

4. Laura has excellent credit. She has two bank credit cards and always pays her bills on time. She applies for instant credit at a major department store to get an additional discount on her purchase, but the clerk tells her that her application was denied. She requests her free annual credit reports at www.annualcreditreport.com to see if she is a victim of identity theft.

Laura is: ☐ savvy ☐ not savvy

5. Andrew is in the military and must obtain a security clearance. Andrew's security clearance is denied because of bad credit—he is advised to check his credit report. When he gets his report, he notices four overdue credit card accounts that he did not open. He calls the credit card companies that issued the accounts and asks to have them closed. He also puts a fraud alert on his account and contacts his superior officer to inform her that he is a victim of fraud.

Andrew is: ☐ savvy ☐ not savvy

Savvy Consumer Quiz Answer Key

1. Erica is **not savvy**. She should never give her personal information over the phone to someone who calls her. Instead, Erica could ask for the caller's number and then hang up and call her financial institution at the phone number on her account statement or on the back of her credit or debit card. If they confirm that the call was not legitimate, Erica should report the number and the suspicious call to the bank's fraud department.

2. Jason is **not savvy**. He should never carry his Social Security card in his wallet. And he should put only the credit cards he needs in his wallet—not all nine of his cards at once.

3. Peter is **not savvy**. He should always go over the credit card statement with Linda to make sure the charges are valid. Otherwise he might pay for unauthorized charges, which he could easily have removed. If he waits more than 60 days from the statement date to dispute unauthorized charges, he may have to pay the whole amount.

4. Laura **is savvy**. Obtaining a credit report is a good way to check if someone else is opening up accounts using her personal information.

5. Andrew **is savvy in some ways**—he checked his credit report and added a fraud alert to stop further damages. He also contacted the credit card companies immediately to close the fraudulent accounts. But he might have been able to stop the fraud—and the credit damage—sooner if he had obtained his free credit reports regularly.

Request for a child's credit report

Equifax	TransUnion	Experian
P.O. Box 105139	PO Box 6790	PO Box 9554
Atlanta , GA 30348	Fullerton, CA 92834	Allen, TX 75013

Date: _____

To: _____

My name is _____. I am the parent/legal guardian of _____, who was born on ___/___/___.

My child's Social Security number is _____. His/her current address is _____.

Within the past 5 years, he/she also lived at (if applicable):

_____.

Please send me a copy of my child's credit report, if one exists. If a record exists, I am requesting that you flag my child's Social Security number with a Minor Alert.

Attached is the required documentation.

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to the fraud department of each of the three credit bureaus. Along with this letter, include the required documentation (for example: a copy of the child's birth certificate and Social Security card; a copy of your driver's license or other government-issued photo identification showing current address; a current utility bill showing your current address). Visit each credit bureau online to find out exact requirements.

Notification of death (to credit reporting agencies)

Equifax	TransUnion	Experian
P.O. Box 105139	PO Box 6790	PO Box 9554
Atlanta, GA 30348	Fullerton, CA 92834	Allen, TX 75013

Date: _____

To: _____

I am writing to request that the credit file for _____ be flagged as "deceased."

His/her most recent address was: _____
His/her Social Security number is _____ and birthdate is___/___/___.

Enclosed please find one copy of the decedent's death certificate. Also enclosed is a copy of a document confirming my authority as the decedent's executor/surviving spouse.

If you have any questions, you may contact me by telephone at _____or by email at _____.

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to each of the three credit bureaus. Along with this letter, include the required documentation (for example: a copy of the death certificate, a copy of the decedent's identification, a copy of your driver's license or other government-issued photo identification, and proof of executorship or marriage). Visit each credit bureau online to find out exact requirements.

To ensure the death is reported promptly to the Social Security Administration, a family member can call the SSA at 800-772-1213 (TTY: 800-325-0778) Mon-Fri from 7:00 a.m. to 7:00 p.m.

Letter notifying existing creditors of identity theft

Date: _____

[Your name]
[Your address]
[City, State, ZIP]

[Your account number]

[Name of creditor]
Attn: Billing Inquiries
[Creditor address]
[City, State, ZIP]

Dear Sir or Madam:

I am writing to dispute a fraudulent transaction on my account in the amount of $_____ on [date] _____. I am a victim of identity theft, and I did not make this transaction. I am requesting that the [charge be removed/the debit refunded], that any finance or other charges that have been assessed as a result of the fraudulent transaction be credited back to my account, and that I receive an updated statement.

Enclosed is a copy of my ID Theft Affidavit explaining the circumstances of the crime.
Please investigate this matter and update my account as soon as possible. You may send any correspondence to the address above.

Thank you.
[Your signature]
[Your name printed]

Instructions:
Fill in blanks with your information. Send by certified mail, return receipt requested, to each creditor where a fraudulent transaction has been processed on your account. Along with this letter, include a copy of your ID Theft Affidavit and police report. If no fraudulent transactions appear on the account, you can modify the letter to serve as simply a notification to the creditor that you are an ID theft victim and that your account may be at risk. The creditor will advise what next steps to take.

Letter requesting records related to fraudulent transaction

Date: _____

[Your name]
[Your address]
[City, State, ZIP]

[Account number or name]

[Name of creditor]
Attn: Billing Inquiries
[Creditor address]
[City, State, ZIP]

Dear Sir or Madam:

As we discussed on the phone on [date] _____, I am a victim of identity theft. The thief made a fraudulent transaction or opened a fraudulent account with your company using my identity. Pursuant to federal law, I am requesting that you provide me, at no charge, copies of applications and other records in your control relating to the fraudulent transaction.

Pursuant to the law, I am providing you with the following documentation, so that you can verify my identity: a copy of my government-issued identification; a copy of the police report; and a copy of my ID Theft Affidavit (form provided by the FTC).

Please provide all information relating to the fraudulent transaction, including: applications, statements, transaction slips, mailing addresses and phone numbers of applicant, investigator's summary, and any other documentation related to the account.

Please send the information to me at the above address and to the officer who is investigating my case: [insert officer's name, address and telephone number].

Thank you.
[Your signature]
[Your name printed]

Instructions:

Fill in blanks with your information. Send by certified mail, return receipt requested, to each company where an account was opened or a transaction was made using your identity. Along with this letter, include a copy of your ID Theft Affidavit and police report. Follow up in 10 days to confirm receipt of the letter and an estimate of when the documentation will be sent to you.

Training Evaluation: *ID Theft & Account Fraud: Prevention & Cleanup*

Please help us improve future presentations by giving us your opinion of today's class. Circle the response that best reflects your feelings about each statement:

1. I have a better understanding what ID theft and account fraud are.

Strongly Agree Agree Disagree Strongly Disagree

2. I know what steps I can take to avoid becoming a victim of fraud.

Strongly Agree Agree Disagree Strongly Disagree

3. I feel confident that I could recognize a scam.

Strongly Agree Agree Disagree Strongly Disagree

4. I have a better understanding of what I should do if I become a victim of fraud.

Strongly Agree Agree Disagree Strongly Disagree

5. I know where to go for more information and assistance on this subject.

Strongly agree Agree Disagree Strongly disagree

6. The instructor was well informed.

Strongly Agree Agree Disagree Strongly Disagree

7. The materials I received are easy to read and understand.

Strongly Agree Agree Disagree Strongly Disagree

8. I would like to attend another class like this.

Strongly Agree Agree Disagree Strongly Disagree

On a scale of 1 to 10 (10 being the highest), how would you rate the seminar? _____

Please let us know how we could improve future trainings (use back, if necessary):

_____

_____

_____

_____

Thank you for attending!