Identifying, Preventing, and Addressing Identity Theft

Lisa Schifferle, Federal Trade Commission
Paula Pierce, Texas Legal Service Center
Keith Morris, Center for Elder Rights Advocacy

Jessica Hiemenz
National Consumer Law Center

National Elder Rights Training Project for the National Legal Resource Center
Sponsorship for this Webinar is provided by the National Consumer Law Center, Elder Law of Michigan, and a grant from the Administration on Aging.
March 9, 2011
• http://www.nlrc.aoa.gov/

• Collaboration developed by the Administration on Aging between the National Consumer Law Center, National Senior Citizens Law Center, American Bar Association Commission on Law and Aging, Center for Elder Rights Advocacy, and the Center for Social Gerontology

• See upcoming trainings, conferences, and webinars
• Request a training
• Request consulting
• Request technical assistance
• Access articles and resources
Moderator – Keith Morris

• Director of the Center for Elder Rights Advocacy, a fellow member of the National Legal Resource Center.
• The Center was established to provide technical assistance to senior legal helplines.
• Keith has managed the Legal Hotline for Michigan Seniors for over eight years and served as a technical assistance resource for other hotlines for the last three years.
Presenter - Lisa Weintraub Schifferle

• Is an attorney in the Federal Trade Commission’s Division of Privacy and Identity Protection.

• At the FTC, she serves on the Identity Theft Team; handles data breach and privacy investigations; and has litigated consumer fraud cases including a work-at-home scam and a foreclosure rescue scam.

• Before arriving at the FTC, Ms. Schifferle spent eight years at the Maryland Legal Aid Bureau, providing direct legal services to low-income residents, as a Staff Attorney and Supervising Attorney.
Presenter – Paula Pierce

• Managing Attorney at Texas Legal Services Center, where she manages the Legal Hotline for Texans, a hotline for Texans aged 60 and older;
• Crime Victim Civil Legal Services, a program that serves elderly and disabled crime victims;
• VICARS, a funded program that provides free legal advocacy for victims of identity theft and financial fraud;
• Self Represented Litigants Project, a project that provides internet based materials for low income persons who cannot afford attorneys.
• For the past ten years her practice has focused on serving the legal needs of the elderly.
Want More Information on Legal Rights and Identity Theft?

New Seventh Edition from NCLC

www.consumerlaw.org
Identifying, Preventing and Addressing Identity Theft

Lisa Schifferle
Federal Trade Commission

Paula Pierce
Texas Legal Services Center
What We Will Cover

- Overview: Understanding Identity Theft and its Victims
- Assisting Victims of Financial Account ID Theft
- Assisting Victims of Non-Financial ID Theft
- Case Study: Using the Pro Bono Manual
- Resources, Tips & Tools for Assisting Victims
Overview

Understanding Identity Theft
Identity Theft

- Identity Theft is when someone uses personal information of someone else to pose as that consumer, in order to
  - fraudulently obtain goods or services in the victim’s name from private and public institutions, or
  - conceal their true identity from authorities or others who perform background checks
Identity Theft and the Elderly

- Identity theft is a form of exploitation. Some states allow a penalty enhancement.
- Three common perpetrators:
  - Relative
  - Caregiver
  - Scammer
- Reporting issues arise when the perpetrator is a relative or caregiver.
- Some cases may trigger a duty to report.
Mrs. S., a retired teacher, fell for a Nigerian email scam.
She wire transferred $1000 to scammers and gave them her PII
Scammer opened a bank account using Mrs. S.’s name and SSN but a different DOB and address (synthetic ID theft).
Scammer used this bank account to receive payments from victims of a fake internet sales scam.
Mrs. S. got a nasty letter from a lawyer threatening to sue her because they thought she was running the internet sales scam.
Id Theft Complaints to FTC (2008)

<table>
<thead>
<tr>
<th>Consumer Age</th>
<th># of Complaints</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 &amp; under</td>
<td>20,597</td>
<td>7%</td>
</tr>
<tr>
<td>20-29</td>
<td>72,637</td>
<td>24%</td>
</tr>
<tr>
<td>30-39</td>
<td>66,809</td>
<td>23%</td>
</tr>
<tr>
<td>40-49</td>
<td>57,745</td>
<td>19%</td>
</tr>
<tr>
<td>50-59</td>
<td>41,969</td>
<td>14%</td>
</tr>
<tr>
<td>60-69</td>
<td>22,197</td>
<td>7%</td>
</tr>
<tr>
<td>70 &amp; over</td>
<td>14,783</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>296,737</td>
<td></td>
</tr>
</tbody>
</table>
What ID Thieves Do with the Information

About 9 million new victims annually

Financial Gain
- Credit Card Fraud 63.5%
- Bank Fraud 33.2%
- Telephone Fraud 15.3%
- Internet Payment Accounts 7.0%
- Medical 4.5%

Concealment
- Given to Police 5.0%
- Employment 1.0%

New Account or SSN misuse: 22%
Existing Account: 92%
The Impact of ID Theft

- Denial of credit
- Loss of credit rating
- Harassment by bill collectors
- Loss/denial of employment
- Lawsuit
- Arrest
- Tax problems
- Garnishment
- Denial of drivers license renewal
- Denial of public benefits
- Denial of medical care
- Time and expense
The Emotional Impact of Identity Theft

Victims may experience:

- embarrassment
- sadness
- helplessness
- anger
- isolation
- betrayal
- rage
- suicidal feelings
Victims may need a lawyer when

- their age, health, language proficiency, or economic situation prevents them from making disputes
- they are sued by creditors attempting to collect debts incurred by an impostor
- they are being harassed by creditors attempting to collect debts incurred by an impostor
- creditors or credit reporting agencies are uncooperative
- to assist with their rights when their identity thief is arrested
- their case is complex or involves non-financial identity theft
Mrs. R., who suffered from advanced dementia, was a private pay resident of an upscale facility. Her care was financed by the rental of her home.

After an absence of several years, her daughter visited regularly for a few months. The visits abruptly stopped. Shortly thereafter, Mrs. R’s monthly payments started to bounce.

Investigators found that the daughter had forged a general durable power of attorney appointing herself as Mrs. R’s personal rep. Using the forged POA, daughter sold Mrs. R’s home, pocketed the sales money & fled.

It was easier to qualify Mrs. R for Medicaid and move her to a less fancy facility than to straighten out the mess made by the daughter.
Assisting Victims of Financial Account Identity Theft
Four Steps Most Identity Theft Victims Need to Take:

1) Contact Consumer Reporting Agencies
2) Contact Companies
3) File a Complaint with the FTC
4) File a Police Report
(1) Contact CRAs

- Place Fraud Alerts on Credit Reports
- Obtain Credit Report *free of charge*
- File Credit Report Information Blocking Request
  - or standard dispute
- Consider Credit Freeze – available under some state laws, or for a fee
  - Prohibits CRAs from releasing the consumer’s credit reports or credit scores without consumer’s authorization
Fraud Alert  vs.  Credit Freeze

- One call
- Creditors must take “reasonable steps” to verify identity
- Less effective
- 90 day, 7 years
- Write each bureau
- No one can apply for new credit – must thaw the report
- More effective
- Effective until thawed
- Possible fee if no police report

No credit? No problem!

Neither will prevent new accounts with merchants that do not check credit reports.
(2) Contact Companies where Thief Committed Fraud

- Contact fraud department, not customer service
- Instruct company to immediately close or freeze the accounts that have been fraudulently opened or used
- Send written dispute including an Identity Theft Affidavit – police report should *not* be required
- Request closure letter from company describing results of their actions
- Request identity theft-related documents
- Ask where to send dispute and document request
(3) File a Complaint with the FTC

- The FTC provides Hotline Phone Counselors and Web-based Consumer Guidance to help victims recover.

- To file an ID Theft Complaint with the FTC:
  - [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 877-438-4338, TTY: 866-653-4261, or by mail.

- Online may print complaint as “ID Theft Affidavit”

- Filing with FTC does not substitute for a report to criminal law enforcement.

- FTC does not take enforcement actions on behalf of individuals.
(4) File a Police Report

- Call the local police as soon as possible
  - Request in-person report filing, leave time to collect documents
  - Request copy of Official Police Report
  - Goal: to get an *Identity Theft Report*

- Some state laws require police to write reports for identity theft victims
  - A map of the states with such laws is at [www.idsafty.org/map](http://www.idsafty.org/map)
Fragile Seniors & Reporting

- Affidavit can be signed by personal representative. Attach copy of POA or Guardianship Letter;
- Any interested person may make a law enforcement report;
- APS report may suffice if you can get proof that a report was made.
After the Four Steps: Correcting the Credit Report

- Fastest and most comprehensive result with “Blocking,” a new consumer’s right under FCRA § 605B
  - Permanently removes the information from credit reports – new accounts, inquiries, etc.
- Alternative: Standard dispute procedures under FCRA § 611
  - Corrects credit report – preserves and corrects valuable existing accounts
Credit Reporting Agencies’ Blocking Obligations - §605B

- Right to permanently suppress identity theft-related information from appearing in credit report.
  - New accounts
  - Inquiries
  - Inaccurate personal information
- CRAs must remove information with four business days after accepting Identity Theft Report
- CRAs must notify furnishers of information that it is result of identity theft
Furnishers’ (Creditors and Debt Collectors) Blocking Obligations

- When furnishers receive *from CRAs* § 605B notice of the block and that the information the furnished resulted from identity theft:
  - Furnishers may not re-furnish that information to any CRA, and
  - Furnishers may not sell, transfer, or place for collection the identity theft-related debt
Credit Reporting Agencies’ Information Dispute Obligations - §611

When a consumer notifies CRA of dispute:

- CRA must send dispute to furnisher of disputed information – often send only a code number
- Furnisher must investigate dispute and report back to CRA – low standards for verifying
- CRA must notify consumer of results of investigation
- If no corrections to credit report, consumer has a right to file a dispute statement
  - 100 words, but CRA can replace with code number
- Must be completed generally in 30 days
Victims’ Rights Under Other Federal Civil Laws

- Fair Credit Billing Act – Limits fraud losses to $50
- Electronic Fund Transfer Act – Limits liability for ATM/Debit transactions – depends on timing notification
- Fair Debt Collections Practices Act – Imposes requirements on debt collectors
- FACTA Amendments to FCRA – Fraud alerts, blocking and business turnover provisions
Assisting Victims of Non-Financial Identity Theft
Medical Identity Theft

- Happens when a thief uses another’s identity or health insurance to receive care
- Dangerous because thief’s medical records become merged with victim’s records
- Difficult to remedy because of HIPAA concerns
Taking SSN off a Medicare Card

- Newer cards are omitting the SSN
- For older cards:
  - Make a copy of the card
  - Black out the SSN with a marker
  - Make a second copy of the card
  - Cut it to wallet size and write the name and phone # of an emergency contact on it
How to Assist Victims

- Report to local law enforcement, get a copy
- Obtain HIPAA compliant authorization forms from victim
- Request medical records from victim’s regular provider as a baseline for comparison
- Request victim’s medical records and privacy policy from each provider that gave care to the impostor. **Important:** Do not mention identity theft at this point.
- Review records, write providers who gave care to impostor requesting correction or segregation and flagging of records. Attach: police report, victim’s ID, relevant portions of genuine records.
- Confirm that records have been corrected and review corrections.
Employment Identity Theft

- Use of victim’s personal identifying information to get or keep employment
- Usually discovered through IRS or denial of public benefits
Example

- Dr. T was a physician who retired to the Rio Grande Valley
- He received a letter from the IRS stating he had not reported income received by working as a dishwasher at a restaurant in a nearby town
How to Assist Victims

- Get a copy of victim’s earnings record from SSA
- Mark impostor activity, provide supporting documentation, request corrected statement
- Provide corrected earnings statement and supporting documents to IRS
- Request that victim’s SSN be flagged
- IRS Identity Protection Specialized Unit: 1-800-908-4490
Clearing Fraudulent Utility Accounts

- Includes electric/gas/water, cable TV, cell phones, landlines, internet, and satellite TV
- Use procedure for clearing fraudulent financial accounts:
  - Send blocking letter to CRA’s if the account appears on victim’s credit report;
  - Send dispute letter and request for account documents to utility provider including copy of victim’s ID, proof of residence, ID theft report, and/or police report + ID theft affidavit
MINIMIZING VICTIMIZATION

- Must change habits to discourage ID theft;
  - Shred!
  - Don’t carry it if you don’t need it;
  - Watch the mailbox;
  - Surf safely;
  - Never give out personal information if you did not initiate the transaction.

- “Sucker lists” and ID sales – victims must remain vigilant, or they will be victimized repeatedly.
Scamproofing our Seniors

Fraud schemes have common themes and follow common patterns.

Single most important question to ask is: **Who initiated the contact?**

If consumer did not initiate the contact, treat it as if it is a scam.
Case Study: Using the Pro Bono Manual

www.idtheft.gov/probono
Case Study: “Jane Doe”

- Jane’s birth certificate and SS card are stolen
- Thief takes job, pays taxes, opens credit cards, and has baby in Jane’s name
- Employment, IRS, financial & medical id theft
- How do you use the Pro Bono Guide to help your client, Jane?
- (note: case study is based on a true story – see http://www.amw.com/fugitives/brief.cfm?id=65654)
### Appendix B.1: List of Sample Questions for Intake Interview

The chart below provides a list of questions you can use to help you understand your client’s situation, particularly if you need to follow up on an incident that your client only briefly mentioned or merely alluded to. The third column indicates which Sections of this guide are likely to apply to the situations listed. We would like to thank the Identity Theft Resource Center ([www.idtheftcenter.org](http://www.idtheftcenter.org)) for allowing us to use its Victim Intake Questionnaire as the basis for this chart.

<table>
<thead>
<tr>
<th>Category</th>
<th>Question</th>
<th>Section(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Were any new credit cards or revolving charge cards opened in your name or using your information?</td>
<td>III.A or B</td>
</tr>
<tr>
<td></td>
<td>Were any of your existing credit cards or revolving charge cards used? Do you still have them in your possession or were they stolen? If they are still in your possession, do you know how the thief obtained the account number(s)? Did you receive a breach notification letter?</td>
<td>III.C.3</td>
</tr>
<tr>
<td></td>
<td>Were any of your ATM or debit cards used? Do you still have them in your possession or were they stolen? If they are still in your possession, do you know how the thief obtained the account?</td>
<td>III.C.2</td>
</tr>
</tbody>
</table>
Use Manual to Gather Background Information

- Tax ID theft - includes Form 14039 & referral to IRS Specialized Unit
- Social Security id theft – advice re: getting earnings statement
- Medical ID theft – advice re: medical records

IV. Addressing Other Forms of Identity Theft
   A. Identity Theft and Children
   B. Criminal Identity Theft
   C. Identity Theft Involving Federal Student Loans
   D. Identity Theft Involving the Internal Revenue Service
   E. Identity Theft Involving the Social Security Administration
   F. Medical Identity Theft
   G. The “Other” Consumer Reports: “Specialty” Consumer Reports
Appendix B.2: Checklist for General Steps Addressing Identity Theft

This checklist walks the victim or her attorney or other representative through the steps she should promptly take to preserve her rights, minimize further harm, and begin to restore her identity. You can use this checklist during the initial interview as a way to identify what steps your client has taken herself so you can chart out the steps that remain to be taken, or at any point during the recovery process to make sure you have taken all appropriate steps to address your client’s particular problems.

1: Steps to Take with the Credit Reporting Agencies
   - Placing Fraud Alerts
   - Obtaining and Reviewing Credit Reports
   - Fixing the Reports

**Placing Fraud Alerts**

- Contact the credit reporting agencies (CRAs) to place an initial 90-day fraud alert. (See Section II.A for more information on fraud alerts and credit freezes.)
  - Issues to consider:
    - Consider placing an extended 7-year fraud alert or a credit freeze on the report immediately.
Sample Letters

- Blocking Request Letters under 605B
- 611 and 623 Dispute Letters
- Letters disputing fraudulent charges
- Letters requesting business records re: identity theft
- Consumer Letters & Attorney Letters
- Attorney follow-up letters
- More than 20 sample letters
Everything in one place

- Manual has copies of the relevant statutes including:
  - FCRA & FACTA Amendments
  - FDCPA
  - Fair Credit Billing Act
  - Electronic Funds Transfer Act
  - Dept of Education regulations
Resources for Assisting ID Theft Victims
Resources


- OVC-Funded Programs:
  - Identity Theft Resource Center (national), 1-858-693-7935, www.idtheftcenter.org
  - Texas Legal Services Center’s VICARS, 1-888-343-4414, www.idvictim.org
  - Maryland Crime Victims Resource Center (statewide victim assistance in Maryland, representation of victims in federal court nationally), 1-877-VICTIMS-1 www.mdcrimevictims.org
  - Atlanta Victim Assistance SAFE campaign (local), 1-404-588-4740, www.atlantava.org
Additional Resources

- Identity Theft Action Center of Nebraska, (402) 880-9596, [www.idtheftne.org/contactus.shtml](http://www.idtheftne.org/contactus.shtml)
- Privacy Rights Clearinghouse, [www.privacyrights.org](http://www.privacyrights.org)
- National Center for Victims of Crime, (202) 467-8700, [www.ncvc.org](http://www.ncvc.org)
- National Crime Victim Law Institute, [www.ncvli.org/](http://www.ncvli.org/) and the Responding to Online Fraud Project contact
  - Meg Garvin ([garvin@lclark.edu](mailto:garvin@lclark.edu) ~ 503-768-6953)
  - Johanna Borkan ([jeborkan@lclark.edu](mailto:jeborkan@lclark.edu) ~ 503-768-6853)
- Department of Justice, Office for Victims of Crime, searchable database of victim service providers, [http://ovc.ncjrs.gov/findvictimservices/](http://ovc.ncjrs.gov/findvictimservices/)
Additional Resources

- ITAC – ID Theft Assistance Center, (referral by member banks to program)
  http://www.identitytheftassistance.org/pageview.php?cateid=50
  - Suspicious activity is detected by victim or financial institution.
  - Financial company refers victim to ITAC.
  - ITAC rep asks victim to fill out an affidavit to document case.
  - Affidavit is shared with other affected account holders (if any), and with victims’ permission, law enforcement.
  - ITAC representative walks victim through their credit report to identify and help correct fraudulent activity.
Additional Resources

- Internal Revenue Service – Identity Protection Specialized Unit, 1-800-908-4490
  - Can Flag File:
    - ID thief may file false tax return for refund claiming to be victim
    - ID thief uses stolen SSN for job, employer reports thief’s income earned to IRS making it appear that victim did not report all income on tax return
  - Taxpayer Advocate Assistance – if eligible, helps those experiencing economic harm, 1-877-777-4778 or TTY/TTD: 1-800-829-4059; See http://www.irs.gov/advocate/article/0,,id=97402,00.html

- Social Security Administration, 1-800-772-1213
  - Only rarely will SSA issue new SSN for victim
  - Quickest way for help is to go to local SSA office
  - Have victim bring ID, SSA card, any documentation showing id theft
  - See www.ssa.gov/pubs/10064.html
Additional Resources

- Pro Bono Guide
- “Guide for Assisting Identity Theft Victims”
Additional Resources

- Identity Theft Victim Assistance Online Training
  www.ovcttac.gov/IdentityTheft

Identity Theft:
Supporting Victims’ Financial & Emotional Recovery

The Office for Victims of Crime (OVC) is pleased to make the e-learning training, Identity Theft: Supporting Victims Financial and Emotional Recovery, available to victim service providers and allied professionals who serve victims of identity theft. All interaction, working with OVC and the Office for Victims of Crime Training and Technical Assistance Center (OVC TTAC), created the e-learning version of the OVC instructor-led training of the same name to make the course more widely available.

Much of the information in this training is based on the document, Assisting Victims of Identity Theft: A Resource Guide for Victim Services, prepared under a grant from the U.S. Department of Justice, Office for Victims of Crime (OVC), and awarded to the Institute for Law and Justice.

OVC would like to acknowledge the following individuals and organizations for their contributions to this project: Paula Pierce, Texas Legal Services Center; Joanna Crane, Federal Trade Commission; Kathleen Claffie, Federal Trade Commission; Debbie Deen, FBI; Linda and Jay Foley, Identity Theft Resource Center; Gus Stiller, Immigration and Customs Enforcement; Donna Hatfield, Immigration and Customs Enforcement; Frank Manion, U.S. Postal Inspection Service; Russell Butler and the MD Crime Victims Resources Center; Sharon Kropf, US Attorneys Office, NY; Jamie Nagy, Identity Theft Action Council of Nebraska; and Savannah Stephens, Atlanta Victim Assistance, Inc. OVC would like to especially acknowledge the victims’ stories of identity theft as told by Vanessa Bustamante, Catherine Culu, Tom Kerr, Nicole Robinson and Andrew Sobaratz. Their stories served as an inspiration in the group’s effort to develop this training for victim assistance providers and allied professionals.

The opinions, findings, and conclusions expressed in this training are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.
Interactive Trainings

Victim Assistance Training Online (VAT Online)
www.ovcttac.gov/vatonline

• 35-40 hour basic victim advocacy web-based training program
• Offers victim service providers opportunity to acquire the basic skills and knowledge they need to better assist victims of crime.
New on the Horizon…

“Expanding Services to Reach Victims of Identity Theft and Financial Fraud”

- OVC E-Pub, [www.ovc.gov](http://www.ovc.gov)
- Recounts Experiences of OVC-Funded Grantees (national, regional, state and local)
- Features Basic Tools and Resources
- “How To” for Developing New and Expanding Existing Services
- Sign Up/NCJRS Registered Users
FTC Disclaimer

- Views expressed in this presentation are not necessarily those of the Commission or any Commissioners.
- Any answers to questions are the opinion of the staff presenter and not the Commission’s or any Commissioner’s.
Contact Information

Lisa Schifferle - FTC
Tel. 202-326-3377
lschifferle@ftc.gov

Paula Pierce
Legal Hotline for Texans
ppierce@tlsc.org
Questions

???