

Title of Training

Date of Training

Facilitators

(SAMPLE – ENTER YOURS HERE)

National Identity Theft Victim Assistance Network

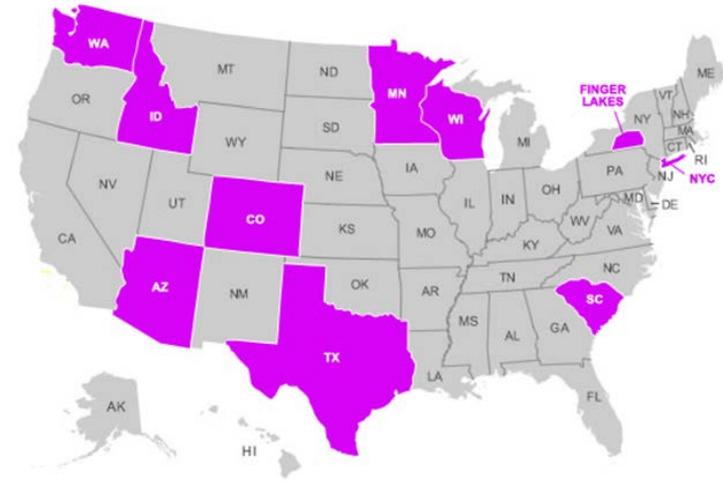
- **Merry O'Brien**, Project Director, NITVAN at the Maryland Crime Victims' Resource Center, merry@mdcrimevictims.org
- **Keith Gethers**, Project Coordinator, NITVAN at the Maryland Crime Victims' Resource Center, keith@mdcrimevictims.org

Washington Coalition of Crime Victim Advocates

- **Rose J. Torgerson**, Director of Training, WCCVA and Project Director, Washington State Identity Theft Alliance, training@wccva.org
- **Shayna Burmeister**, Director of Outreach, WCCVA and Project Director, Washington State Identity Theft Alliance, admin@wccva.org

National Identity Theft Victim Assistance Network

- Funding: U.S. Dept. of Justice, Office for Victims of Crime (OVC).
- The existing victim support network is limited in infrastructure, coordination, & training to assist ID theft victims.
- By creating a national network of 10 coalitions, project seeks to build field's capacity, help provide a coordinated response to problem, improve outreach & capacity of programs to better address ID theft victims' rights & needs.
- Goals and Activities of the Coalitions:
 - Awareness: Community outreach/public awareness campaigns
 - Professional Education: training of service professionals in region
 - Systems-Change: improved inter-agency infrastructure, coordination, referrals



Part of a Large & Diverse Network



- **Arizona Identity Theft Coalition** coordinated by AZ Attorney General's Office
- **Identity Theft Advocacy Network of Colorado** coordinated by CO Bureau of Investigation
- **Finger Lakes (NY) Identity Theft Coalition** coordinated by Lifespan
- **Idaho Coalition Against Identity Theft** coordinated by ID Legal Aid Services
- **Minnesota Identity Theft Coalition** coordinated by BWLAP
- **NYC Identity Theft Coalition** coordinated by South Brooklyn Legal Services
- **South Carolina Identity Theft Network** coordinated by SC Victim Assistance Network
- **Texas Identity Theft Network** coordinated by TX Legal Services Center
- **Washington Identity Theft Alliance** coordinated by WA Coalition of Crime Victim Advocates
- **Wisconsin Identity Theft Network** coordinated by Coalition of WI Aging Groups



IDENTITY THEFT VICTIMS
ASSISTANCE NETWORK PROJECT

Identity Theft Training

This training was produced by the National Identity Theft Victims Assistance Network under award # 2010-VF-GX-K030, awarded by the Office for Victims of Crime, Office of Justice Programs, U.S. Department of Justice.

The opinions, findings, and conclusions or recommendations expressed in this document are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Part I

The Crime:

What is Identity Theft
and What Impact Does the
Crime Have on Victims?

Objectives

Participants will be able to:

1. Define identity theft, the many forms of financial and non-financial identity theft, and related financial crimes
2. Understand the impact of the crime on victims;
3. Identify the initial and long-term steps in assisting victims in recovery after an identity theft.

Identity Theft: Federal Law

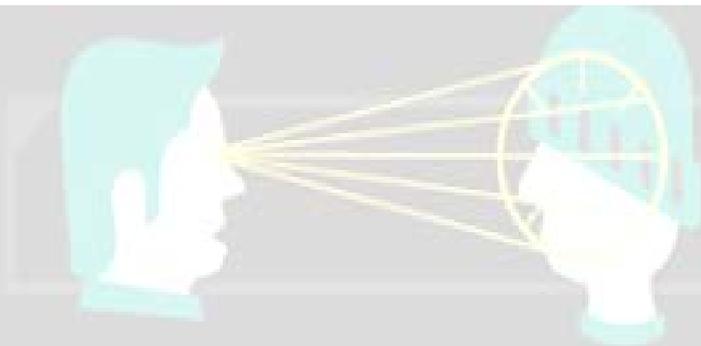
- The use or attempt to use personal information of another person to commit fraud.
- Defined in the Fair Credit Reporting Act (FCRA):
 - “Identifying information” is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person . . .

State ID Theft Laws (SAMPLE, ENTER YOUR STATE'S HERE – YOU CAN FIND YOUR STATE'S LAWS AT: identitytheftnetwork.org/resource-map

**No person may not:
knowingly obtain, possess, use, or transfer
a means of identification or financial
information of another person,
living or dead, with the intent to commit,
or to aid or abet, any crime.**

How Does Identity Theft Occur?

1. Dumpster Diving
2. Skimming
3. Phishing
4. Changing Address
5. Old-Fashioned Stealing
6. Pretexting
7. Hacking
8. ID Assumption



Interestingly, in **43%** of identity theft cases, the victim knew the criminal.

Types and Methods of ID Theft Deployed Commonly

- Medical ID Theft
- Criminal ID Theft
- Employment Fraud
- Benefits Fraud
- Account Takeover
- Credit Card/ATM Misuse
- Dumpster Diving
- Phishing
- Changing Address
- Old-Fashioned Stealing
- Pretexting
- Hacking
- ID Assumption
- Coercion
- Undue influence & abuse of legal authority (POA's)



Financial Identity Theft

The most common form of identity theft involves the fraudulent use of a victim's personal info for financial gain.

1. the use of the victim's existing credit, bank or other accounts; or
2. the opening of new accounts in the victim's name.

Non-Financial Identity Theft

- Criminal Identity Theft
- Governmental Fraud
 - ❖ IRS tax fraud
 - ❖ Social Security Administration
 - ❖ Dept. of Social Services
- Synthetic Identity Theft
- ID Theft Assumption
- Medical Identity Theft

Non-Financial: Medical Identity Theft

- FBI director Louis Freeh: *"We have seen cocaine distributors switch from drug dealing to health care fraud schemes. The reason - the risks of being caught & imprisoned are less."*
- Can alter:
 - Medical file history
 - Insurance rates and limit caps
 - Credit reports (collections)
 - Employment chances & issues with law enforcement
- Perpetrators? addicts, career criminals, sick people & their families
- Monitoring credit not very useful until collections actions

Identity Theft and the Big Picture: The Impact of Victimization

How Does Identity Theft Affect Victims?

Over 3 million identity theft victims experienced issues such as:

- having utilities cut off;
- being arrested;
- finding erroneous claims on their health records and
- being harassed by collection agencies.

How Does Identity Theft Affect Victims?

53% of ID theft victims feel moderate to severe distress from the identity theft.

- Why did this happen to me?
- The police don't care
- Anger/Frustration
- Vulnerable/Violated
- Helpless/Stressed
- Depressed
- Suicidal



Langton, L. & Planty, M. (2010).
Bureau of Justice Statistics
Special Report, National Crime
Victim Victimization Survey
Supplement, Victims of Identity
Theft 2008.

Seniors Can Be Hit Hard

- Much harder time recovering financially than younger wage earners.
- 1 in 10 must turn to Medicaid after their funds are stolen, moving out of community into nursing homes.
- \$2,600,000,000 per year lost to financial crimes against seniors in the U.S.



Part II

The Recovery: How to Assist Victims After Identity Theft Occurs

Basic Steps for ID Theft Recovery

Identity Theft Affidavit

- Provides critical info in comprehensive, standardized manner
- Can be used in disputes with creditors, credit reporting agencies – widely accepted
- Start with the FTC online complaint www.ftc.gov/idtheft or via phone
 - Gather info first - credit reports, billing statements, collection letters
 - Include as much detail as possible
- Print complaint, “ID Theft Affidavit”

Identity Theft Complaint Process



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

[Privacy Policy](#) | [Federal Trade Commission](#)

FTC Complaint Assistant

Step 1

Step 1: Let's Get Started

Welcome to the FTC Complaint Assistant. So that we can properly record your complaint, you will first be asked to answer a series of questions. After answering these questions, you will have the opportunity to provide us additional details regarding your complaint in your own words. Please start by telling us how we can best contact you.

Contact Information

First Name:

Last Name:

Identity Theft Affidavit Form

Average time to complete: 10 minutes

Identity Theft Victims' Complaint and Affidavit

A voluntary form for filing a report with law enforcement and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You (the victim)

Now

- (1) My full legal name: _____
First Middle Last Suffix
- (2) My date of birth: _____
mm/dd/yyyy
- (3) My Social Security number: _____ - _____ - _____
- (4) My driver's license: _____
State Number
- (5) My current street address:

Number & Street Name Apartment, Suite, etc.

City State Zip Code Country
- (6) I have lived at this address since _____
mm/yyyy
- (7) My daytime phone: (____) _____
My evening phone: (____) _____
My email: _____

This section is for the victim's information, even if he or she cannot complete the form.

Leave (3) blank until you provide this form to someone with a legitimate business need, such as when you are filing your report at the police station or sending the form to a consumer reporting company to correct your credit report.

At the Time of the Fraud

- (8) My full legal name was: _____
First Middle Last Suffix
- (9) My address was: _____
Number & Street Name Apartment, Suite, etc.

City State Zip Code Country
- (10) My daytime phone: (____) _____ My evening phone: (____) _____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

Washington Mandatory Police Reports for IDT Victims (SAMPLE – find your state at: identitytheftnetwork.org/resource-map)

A person who has learned or reasonably suspects that his or her financial information or means of identification has been unlawfully obtained, used by, or disclosed to another, may file an incident report with a law enforcement agency, by contacting the agency that has jurisdiction over his or her actual residence, place of business, or place where the crime occurred.

The agency must create a police incident report of the matter and provide the complainant with a copy of that report. The law enforcement agency may refer the incident to another law enforcement agency, and the law does not require the law enforcement agency to investigate the reports of identity theft.

In addition, identity theft incident reports are not required to be counted as an open case for purposes of compiling open case statistics.

Identity Theft Report

- Identity Theft Report is a report:
 - A. that alleges an ID theft,
 - B. that is a copy of an official, valid report filed by a consumer with an appropriate Federal, State, or local law enforcement agency
- When victim completes the complaint process, creating the ID Theft Affidavit, the details can assist law enforcement in ensuring sufficient detail is available to create the Crime Report.

Identity Theft Report Benefits

- 1. Blocking fraudulent info from appearing on credit report**
- 2. Preventing a company from refurnishing fraudulent info to a CRA**
- 3. Preventing a company from selling or placing for collection bad debts that result from ID theft**
- 4. Placing an Extended Fraud Alert:** need an ID Theft Report to place an extended 7-yr fraud alert on credit reports.
- 5. Obtaining transaction docs from businesses**

Assisting Victims of Financial Identity Theft

Addressing Account-Related ID Theft

Tools:

1. Fraud Alerts
2. Credit Freezes
3. Blocking Information

Some of these tools require an ID Theft Report

- FTC Complaint/Affidavit AND
- Police Report

**Each law discussed in the following portion of the presentation
is provided, in full, in the training packet.*

Financial Identity Theft: Immediate Steps to Recovery

1. Contacting Companies/Close Accounts
2. Contacting Credit Reporting Agencies (CRAs)
3. Filing a Complaint with the FTC
4. Filing a Police Report

Long Term Steps to Recovery

1. Consider an **Extended Fraud Alert**
2. Consider **Credit Freeze**
3. Obtain Copies of Credit Report
 - **Monitor** Credit Reports
 - **Blocking Information:** Disputing Fraudulent accounts and transactions by correcting reports

Extended Fraud Alert

- Lasts for 7 yrs.
- Major difference between an initial alert
- CRAs must remove victim's name from marketing lists for pre-screened credit offers for 5 yrs.
- Entitled to 2 free credit reports within 12 months from each of the 3 nationwide CRAs
- *Requires ID Theft Report*

Washington's Credit Freeze Law (SAMPLE – find your state at: identitytheftnetwork.org/resource-map)

- All WA consumers can place freezes on credit reports to prevent new accounts from being opened in their names.
- Only victims of id theft are permitted to place a freeze on their accounts.
- Must request by certified mail.
- CRAs may charge \$10. However, id theft victims with a report or 65+ seniors not charged.
- CRA must place freeze within 5 business days after receiving request & within 10 days provide password for consumer when providing authorization for release of credit for a specific party or period of time.

What a Fraud Alert and Credit Freeze *Won't* Do

- Won't Stop Ongoing Fraud
- Won't Protect Existing Accounts
- Won't Prevent Non-Financial Account Fraud
 - Many companies, such as medical providers, utilities, banks do not check credit report before providing services, opening accounts
 - Concealment, Rental, Employment Fraud likely not prevented

Remedies

- **Blocking Errors in Credit Reports**
Using FCRA § 605B
- **Disputing Errors in Credit Reports**
Using FCRA Sections 611 & 623
- **Disputing Credit Card Charges**
Using FCBA 15 U.S.C. § 1601
- **Disputing Debts**
Using FDCPA 15 U.S.C. § 1692
- **Disputing ATM & Debit Card Transactions**
Using Electronic Fund Transfer Act (EFTA)
- **Restitution**
Identity Theft Enforcement & Restitution Act of 2008

Summary of Rights of Identity Theft Victims

- Right to file identity theft report.*
- Right to place fraud alert on credit report.*
- Right to free credit report.*
- Get documents relating to the identity theft.*
- Right to a credit report free of fraudulent accounts.*
- Right to stop debt collectors from contacting to collect on fraudulent debts. **

*Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 and FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

**THE FAIR DEBT COLLECTION PRACTICES ACT, as amended by Public Law 104-208, 110 Stat. 3009 (Sept. 30, 1996)

Resources to Minimize Re-Victimization

- www.Onguardonline.gov
Site has interactive games to help senior be a smarter consumer on issues of related to spyware, lottery scams, etc.
- www.Donotcall.gov (1-888-382-1222)
Seniors register phone number to stop solicitation calls except from political & charitable organizations.
- Tip Sheet as a Handout (Included in CD and snapshot below):

1. Be aware that you're at risk from strangers—and from those close to you.
2. Do not isolate yourself—stay involved!
3. Always tell solicitors: "I never buy from (or give to) anyone who calls or visits me unannounced. Send me something in writing."
4. Shred all receipts with your credit card number.
5. Sign up for the "Do Not Call" list (1-888-382-1222) and take yourself off multiple mailing lists.
6. Use direct deposit for benefit checks.
7. Never give your credit card, banking, Social Security, Medicare, or other personal information over the phone unless you initiated the call.
8. Be skeptical of all unsolicited offers.

Assisting Victims of Non-Financial Identity Theft

Employment Identity Theft: How to Assist Victims

- Get a copy of victim's earnings record from SSA
- Mark impostor activity, provide supporting docs, request corrected statement
- Provide corrected earnings statement & supporting docs 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 & satellite TV, cell phones, landlines, internet
- Procedure for clearing fraudulent accounts:
 - Send blocking letter to CRA's if account appears on victim's credit report;
 - Send dispute letter & request for account docs to utility provider including copy of victim's ID, proof of residence, ID theft report, and/or police report + ID theft affidavit

Medical Identity Theft

- Leader in issue & solution - World Privacy Forum : www.worldprivacyforum.org
- “Victims do not have clear pathways for recourse and recovery. For example, victims do not have the legal right to demand correction of their medical information that was not created by the provider or insurer currently maintaining or using the info. This circularity can make it impossible for a medical identity theft victim to erase false entries from a medical or insurance record. This is true even when false entries were put in the record during the commission of a crime, such as health care fraud or medical identity theft.” – WPF
- HIPAA

Part III

Resources

Reference Resource: FTC Website

[Back to FTC.gov](#)

[Report ID Theft](#) | [Order Free Resources](#) | [Privacy Policy](#) | [Get Email Updates](#)

**FIGHTING BACK AGAINST
IDENTITY THEFT**
FEDERAL TRADE COMMISSION



[CONSUMERS](#)

[BUSINESSES](#)

[LAW ENFORCEMENT](#)

[MILITARY](#)

[MEDIA](#)

[REFERENCE DESK](#)

[EN ESPAÑOL](#)

DEFEND: RECOVER FROM IDENTITY THEFT

Take steps to respond to and recover from identity theft as soon as you suspect it.

[What are the steps I should take if I'm a victim of identity theft?](#)

[What is a fraud alert?](#)

[What is a credit freeze?](#)

[What is an identity theft report?](#)

[What do I do if the police only take reports about identity theft over the Internet or telephone?](#)

[What do I do if the local police won't take a report?](#)

[How do I prove that I'm an identity theft victim?](#)

[Should I apply for a new Social Security number?](#)

What are the steps I should take if I'm a victim of identity theft?

If you are a victim of identity theft, take the following **four steps** as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name.

Hot Links

**Guide for
Assisting
Identity Theft
Victims**



[Watch the video](#)

[Use Our Materials In Your
Community](#)

Case Study: PEACE Coalition - Protecting Elders Against Crime & Exploitation



1. Increase public awareness
2. Educate professionals who come into contact with seniors
3. Increase referrals & partnerships amongst agencies in order to better serve senior victims
4. Advocate for policies to protect seniors

Training Resource: Online Victim Advocate Course

OVC Identity Theft Victim Assistance Online Training Supporting Victims' Financial and Emotional Recovery



OVC'S NEWEST E-LEARNING TOOL

This online training provides advocates and other allied professionals with the tools they will need to better understand the rights and needs of this underserved category of victims and to help assist victims of identity theft in their financial and emotional recovery. It includes:

- A wealth of information about the various types of identity theft, laws that support victims' rights, as well as referral agency and resource information to better serve victims of identity theft.
- Engaging case studies to provide victim advocates with opportunities to interact with victims of identity theft through the path to recovery.



Network Support Resource: NITVAN Website



FIND

[Login](#) | [Register](#) | [Contact](#)

NATIONAL PROJECT

NETWORK OF COALITIONS

COLLABORATE

SERVE VICTIMS

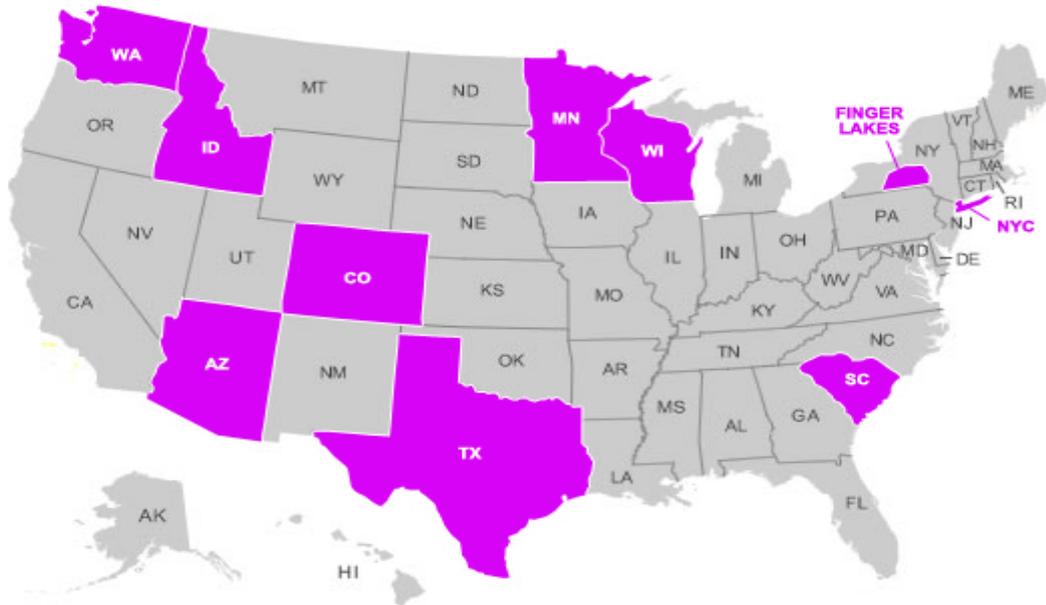
GET HELP

MEMBERS

Resource Map

Click on a state on the map below to learn more about its:

State Criminal Laws • State Laws for Expunging Criminal Arrest Records • State Laws for Credit Information Blocking • State Laws Regarding Social Security Numbers • State Laws for Security Freezes • State Laws on ID Theft Passports



NEWS FEED

[New Survey Shows Sizable Gap Between Americans' Online Security Perceptions and Actual Practices](#)

WASHINGTON, Nov. 15, 2011 Many Don't Follow Common Cyber Security [...]



[NYC Hotel Auditor Indicted in Guest Credit Card Scam](#)

November 15, 2011. An auditor for a stylish New York [...]



[Family Secrets: Parents Prey On Children's Identities As Victims Stay Silent](#)

November 15, 2011. Originally published on Huffington Post "Burdened Beginnings" [...]



Find us on Facebook



Identity Theft Network

Like 199



Several Additional Resource-Rich Websites

1. **Better Business Bureau**
2. **Identity Theft Resource Center**
3. **Social Security Administration**
4. **US Postal Administration**
5. **Credit Bureaus: Equifax, Experian, TransUnion**
6. **AnnualCreditReport.com**
7. **National Center on Elder Abuse (NCEA)**
8. **The National Committee for the Prevention of Elder Abuse (NCPEA)**
9. **AARP Foundation**