

Mental Health Issues in Identity Theft

Identity Theft

Module 1 – Identity Theft 101

Learning Objectives for Module 1

1. Define identity theft.
2. Describe ways personal information is acquired and used by identity thieves.
3. Describe steps for victims to take to recover their identity and repair their credit.
4. Identify resources available to victims.

This was produced by the Texas Identity Theft Coalition, Texas Legal Services Center, and Trauma Support Services of North Texas under Sub-award funding from the Maryland Crime Victims Resource Center, Inc. (MCVRC) under Cooperative Agreement No. 2010-VF-GX-K014, 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 herein are those of the contributors and do not necessarily represent the official position or policies of the U.S. Department of Justice or of the MCVRC.

True or False

- Data breach is a form of ID theft.
- Brownsville, Texas is a national ID theft hotspot.
- An estimated 5 million Americans were victimized by identity thieves in 2009.
- A felon can exit prison with a clean criminal history.
- More ID theft happens by computer hacking than through old fashioned stealing or dumpster diving.

What is Identity Theft?

The theft or misuse of personal identifying information in order to gain something of value or facilitate other criminal activity.

Texas Definition

Texas Penal Code § 32.51:

**to obtain, possess, transfer, or use a person's
“identifying information” or
“telecommunication access device” with the
intent to harm the person.**

What information is stolen:

Personal information that can be used to commit identity theft includes:

- Name
- Social Security Number
- Address
- Date of Birth
- Telephone number
- Biometric data
- Financial account numbers or access cards
- Passwords, Mother's maiden name, Father's middle name, answers to "challenge" questions

How is information stolen?

Low Tech

- Trash diving
- Lost/stolen wallet/purse
- Mail theft
- Burglary

High Tech

- Skimming
- War driving
- Computer hacking
- Data breach
- Scams/fraud

What Thieves Do with PII

Existing Accounts

- Bank
- Credit Card
- Utility

New Accounts

- Bank
- Credit Card
- Utility
- Loans

Non-Financial

- Medical
- Employment
- Criminal
- Government benefits

Identity Theft and Other Crimes

- Domestic Violence
- Sexual assault, assault, burglary, robbery
- Homicide
- Terrorism
- Drug Trafficking

Victim Experiences

- Denial of credit
- Loss of credit rating
- Harassment by bill collectors
- Loss/denial of employment
- Lawsuit
- Arrest
- IRS problems
- Garnishment
- Denial of drivers license renewal
- Denial of public benefits
- Denial of medical care

ASSISTING VICTIMS

TLSC's Victim Toolkit

Download free from www.idvictim.org

▸ Home

▸ About Us

▸ Contact Us

▸ **Victim's Toolkit**

▸ Resources

▸ News

▸ Links

▸ Upcoming Events

▸ Frequently Asked Questions

▸ TexasLawHelp.org

VICARS

Victims Initiative for Counseling, Advocacy, and Restoration
of the Southwest

1-888-343-4414

We help Texas residents who are victims of
identity theft:

- Re-acquire their identity
- Restore their credit
- Recoup their losses
- Regain control over their finances

Disclaimer | Admin Login

powered by **probono.net**

IMMEDIATE CONCERNS

- **Stop impostor activity**
- **Report the crime**
- **Repair the damage**

Preparation

- Toolkit pages 1-4
- Victims feel like they are treated as criminals because they are constantly asked to identify themselves and repeat the facts of the theft.
- Victims are less frustrated when they understand what will be required.
- Victims are more successful when they have written down important facts so that they can recite them quickly and accurately.
- Encourage victims to write down the time spent – in case they can request restitution later.

Stopping the Bleeding

- Call businesses and report the fraud;
- Renumber or close existing accounts;
- If a bank account is compromised, ask bank to put the account in the CANS;
- Replace credit cards
- Get a fraud alert



Fraud Alerts

- Initial: 90-day, renewable, one free credit report
- Extended: 7-year, need ID Theft Report, two free credit reports
- Set fraud alert by contacting *only one* of the three CRAs
 - Equifax 800-525-6285
 - Experian 888-397-3742
 - TransUnion 800-680-7289
- Must provide personal information to match file
- Beware of diversion to “free annual report” or other commercial services during call

Fraud Alert vs. Credit Freeze

- One call
- Less effective
- 90 day
- 7 years (police rpt.)

- Write each bureau
- No new credit
- More effective
- No expiration
- Fee w/o police rpt.

**NO
CREDIT CHECK**

Helpful Intake Questions:

- How did you find out your identity was stolen? (Example: I was turned down for a car loan.)
- When did you find out your identity was stolen?
- What was taken or misused and in what amounts?
- Were new accounts opened?
- Do you have written proof? (Example: letter from a debt collector)

How to Get a Free Credit Report

www.annualcreditreport.com

Equifax	800-525-6285 P.O. Box 740241 Atlanta, GA 30374
Experian	888-397-3742 P.O. Box 9532 Allen, TX 75013
Transunion	800-680-7289 P.O. Box 6790 Fullerton, CA 92834
Innovis www.innovis.com	1-800-540-2505 P.O. Box 1358 Columbus, OH 43216



Reporting ID Theft

- Federal Trade Commission (www.ftc.gov)
- Local police or sheriff
- Usually NOT FBI, but instead . . .
- Secret Service
- U.S. Postal Inspectors
- IC3

Crucial Document: The Identity Theft Report

What is it?

A law enforcement report that shows that the crime was reported and that contains enough information about the crime that CRAs and businesses can substantiate the ID theft.

How to get one

In Texas, you won't. The public portion of our police reports does not contain enough information to serve as an IDT Report under the FCRA.

So, what's a consumer to do?

Make a report to the FTC on the website. Print it, sign it in front of witnesses or a notary. This becomes an identity theft affidavit. Attach it to the police report.

Clearing Accounts

Two step process:

1. Credit reporting agencies aka credit bureaus
2. Businesses that gave credit, services, or goods to the identity thief

BIGGEST CONSUMER MISTAKE: Failing to follow-up in writing!

Credit Reporting Agencies

FCRA gives consumers rights to:

1. Block fraudulent info from credit report and
2. Have credit reporting agencies notify creditors of the fraud

MUST BE IN WRITING and attach:

1. Copy of identity theft report or
2. Copy of police report or proof of report and ID theft affidavit
3. Copy of government issued ID (drivers license, etc.)

Sample letters available at www.idvictim.org or www.idtheft.gov/probono

Businesses

FCRA gives consumers the right to get a copy of fraudulent account records and prevents creditors from placing a disputed account with a debt collector.

MUST BE IN WRITING and attach:

1. Copy of identity theft report or
2. Copy of police report or proof of report and identity theft affidavit and
3. Copy of government issued ID (drivers license, etc.)

Sample letters available at www.idvictim.org or www.idtheft.gov/probono.

Tips for Victims

- If it's not in writing, it doesn't count – get confirmation!
- Send everything certified mail, return receipt requested; by fax; by email with scanned attachments; or other method where you can prove it was received.
- Be ready to repeat ... and repeat ... and repeat!
- Businesses have a financial incentive to give victims the runaround. Be precise. Include the attachments. Be tenacious. Be persistent. If all fails, report the business to the FTC, www.ftc.gov.

NON-FINANCIAL ID THEFT

Medical ID Theft:

How to Assist Victims

- Report to local law enforcement, get a copy
- Victim requests medical records from own doctor
- Request victim's medical records from providers that gave care to the thief. **Important: Do not mention identity theft at this point.**
- Write providers who gave care to the thief requesting correction or segregation and flagging of records. Attach: police report, victim's ID, relevant portions of genuine records.
- Confirm in writing that records have been corrected and review corrections.

Employment ID Theft: How to Assist Victims

- Get a copy of victim's earnings record from SSA
- Mark items that are not the victim's, 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

Criminal ID Theft: How to Assist Victims

- Texas Stolen Identity File:
 - Local sheriff takes photo and fingerprints
 - Verifies that victim is not the criminal
 - Submits to DPS
 - Victim receives confirmation letter and password
- If crime is in another state, contact law enforcement there, provide proof of victim's identity and alibi information, request letter of clearance.
- Provide letter of clearance to relevant businesses, agencies, and data brokers.

Application to be Declared a Victim of ID Theft

Bus. & Comm. Code Sec. 521.101-521.105

- ID theft victims may apply to District Court to be declared a victim of ID theft;
- Even if doesn't know identity of thief;
- Burden of proof is preponderance of evidence;
- Order must be sealed;
- Order may be vacated if obtained fraudulently.

WHEN THE THIEF IS CAUGHT

- Less than 1% of cases
- No right to CVC in most states; although, not prohibited by federal law
- Some locales argue that Crime Victims' Bill of Rights does not apply to ID theft victims (not a violent crime)
- Victim should provide a written VIS
- If victim desires, should be permitted a chance to speak at sentencing

Friendly Contact Keeps Victims On Track!

- Follow-up phone calls
- Friendly reminders
- Look for signs that victim needs:
 - Medical attention
 - Attorney or
 - Extra help
- Make referrals

MINIMIZING RE-VICTIMIZATION

- Shred!
- Watch the mailbox;
- Surf safely;
- Don't carry it if you don't need it;
- Never give out personal information if you did not initiate the transaction.

How to Monitor Credit for Free

- FCRA gives consumers one free credit report per year from each of the three bureaus.



In:	Order from:
January	Equifax
May	Experian
September	Transunion

Resources

- Federal Trade Commission, www.ftc.gov/idtheft, 1-877-ID-THEFT; <http://bulkorder.ftc.gov> to order consumer education materials; pro bono guide, www.idtheft.gov/probono
- Texas Legal Services Center's VICARS
1-888-343-4414, www.idvictim.org
- Identity Theft Resource Center (national),
1-858-693-7935, www.idtheftcenter.org
- Maryland Crime Victims Resource Center (statewide victim assistance in Maryland, representation of victims in federal court nationally through referrals), 1-877-VICTIMS-1;
www.mdcrimevictims.org
- Identity Theft Victim Assistance Online Training through OVC-TTAC, <https://www.ovcttac.gov/identitytheft/>

Additional Resources

- Expanding Services to Reach Victims of Identity Theft and Financial Fraud, an e-publication of the OJP,
http://www.ojp.usdoj.gov/ovc/pubs/ID_theft/pfv.html
- Department of Justice, Office for Victims of Crime, searchable database of victim service providers,
<http://ovc.ncjrs.gov/findvictimservices/>
- IRS Identity Protection Specialized Unit,
1-800-908-4490

Additional Resources

- Texas Attorney General's consumer scam page, www.oag.state.tx.us/consumer/scams.shtml
- Snopes, www.snopes.com/fraud/topscams.asp
- IC3 scams page, www.ic3.gov/crimeschemes.aspx
- Safe surfing tips, <http://onguardonline.gov/>;
<http://www.cyber-safety.com/>

Author's Contact Information

Paula Pierce

Manager of Hotline Programs, Texas Legal
Services Center

815 Brazos, Suite 1100

Austin, TX 78701

Phone: 888-343-4414

Email: ppierce@tlsc.org