



Identity Theft:

El Paso ISD Presentation

October 3, 2011

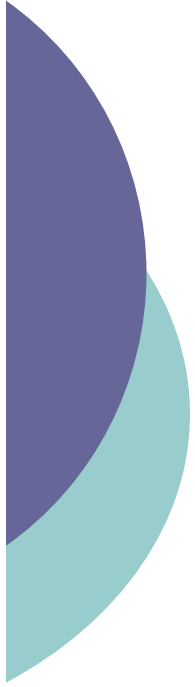
Deanya T. Kueckelhan
Southwest Region - Dallas

FEDERAL TRADE COMMISSION
Protecting America's Consumers



What We Will Cover

- Understanding Identity Theft
- Assisting Victims of Financial Account ID Theft
- Assisting Child ID Theft Victims
- Resources, Tips & Tools for Assisting Victims




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



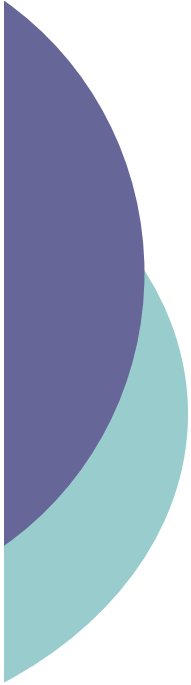
What ID Thieves Do with the Information FTC 2010 Survey (for years 2008 to 2010)

- Government documents or benefits Fraud 19%
- Credit card Fraud 15%
- Phone or utilities Fraud 14%
- Employment Fraud 11%
- Loan Fraud 4%
- Other 22%
 - Internet or Email Fraud
 - Medical Fraud
 - Insurance Fraud
 - Child Support
 - Bankruptcy

Texas Overview

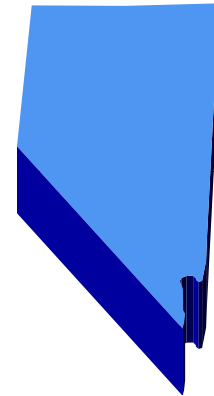


- Texas is in the middle for the number of fraud complaints reported to FTC (#29). Not too bad...
- But...Texas is the **5th** leading state in the number of identity theft complaints reported to the FTC
 - Over 24,000 complaints in 2010
- Texas has **8** metro areas in the top 50 for ID theft complaints: El Paso is #15.



Texas Identity Theft Statistics

1 Government Doc/Benefits Fraud	22%
2 Employment-Related Fraud	21%
3 Phone or Utilities Fraud	13%
4 Credit Card Fraud	11%
5 Bank Fraud	10%
6 Loan Fraud	4%
Other	20%
Attempted Identity Theft	5%





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:

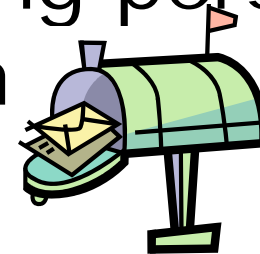
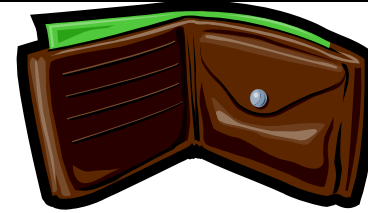
- embarrassment
- sadness
- helplessness
- anger
- isolation
- betrayal
- rage



How does identity theft happen?

Old-fashioned identity theft

- Lost or stolen wallets
- Theft by family or friends
- Dumpster diving – obtaining personal information from the trash
- Stolen mail
- Buying it from a corrupt insider at a bank, hotel, car rental agency, or other business





New, high-tech identity theft

- Skimming
- Data breaches
- Phishing
- Keystroke loggers and malicious code
- Peer-to-peer file sharing



Skimming

- The copying of electronically transmitted data on the magnetic strip of a credit card, to enable valid electronic payment authorization to occur between a merchant and the issuing financial institution.



Skimming

○ Common Skimming Locations

- Restaurants
- Hotels
- Gas Stations (affixed to pumps)
- ATMs (affixed to machine)







Data Breaches

Breaking into computer systems

- Intruders need find only the weakest link:
 - Vulnerable system
 - Unsecured network
 - Disgruntled or corrupt insider – Once inside, often free to search and steal data



Phishing

- Sending authentic-looking but fraudulent e-mail designed to trick the respondent into giving out sensitive personal information



Deterring Identity Theft



Deter ID thieves from stealing your personal information

- **Empty** your purse or wallet (SSN cards)
- **Shred**
- Don't give out your personal information unless you are sure who you are dealing with
- Keep personal information **secure** – home, car, office
- **Monitor** accounts and review financial statements regularly
- Get your free annual credit report at www.annualcreditreport.com



Deter thieves from stealing your personal information online

- Keep anti-virus software up-to-date
- Be careful using social networks (e.g., Facebook, Google+) or peer-to-peer file sharing software.
- If you have online accounts, use difficult to guess passwords
- When online shopping look for indications that the site is secure
- Don't click on links in unsolicited emails



Assisting Victims Identity Theft



Four Steps Most Identity Theft Victims Need to Take:

- 1) Contact Consumer Reporting Agencies (CRAs)
- 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*
- 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



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



3) File a Complaint with the FTC

- To file an ID Theft Complaint with the FTC:
 - 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 your local police as soon as possible
 - Request copy of Official Police Report
- Some state laws require police to write reports for identity theft victims
 - A map of the states with such laws is at www.idsafety.org/map



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 within four business days after accepting Identity Theft Report
- CRAs must notify furnishers of information that it is result of identity theft



Creditors and Debt Collectors (furnishers) Blocking Responsibilities:

- 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



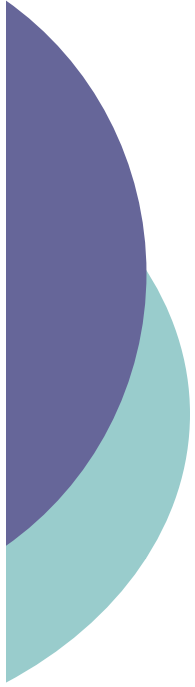
Victims' Rights Under Other Federal Civil Laws

- 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



Clearing Utility Account Fraud

- 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



Assisting Child

Identity Theft Victims



Overview

- Carnegie Mellon CyLab Study:
 - 40,000 U.S. children
 - 10.2% of children in the study had someone else using their SSN – 51 times higher than the 0.2% for adults
 - 75% involved malicious fraud (24% were mixed credit file info)



Foster Care Identity Theft

- Unlike kids who can turn to parents to help them correct credit errors, foster kids generally don't have "family advocates" to help them with this
- Unless specifically directed to do so, their "legal custodian" – the state or county child welfare agency – would likely not look into their credit problems, even during their "transition period" before emancipation
- If a youth only learns about the theft of their identity after they emancipate from foster care, it can negatively affect their successful transition to adulthood



Familial Identity Theft

- When family steals child's identity, it's often harder to correct
 - Family member who would usually be the one to help may be the perpetrator
 - Poverty-related issues (will stopping the identity theft cause greater harm to child?)
 - What if child does not want to file police report against family member?



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>)

Intake - Checklist

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) for allowing us to use its Victim Intake Questionnaire as the basis for this chart.

Category	Question	Section(s)
Financial	Were any new credit cards or revolving charge cards opened in your name or using your information?	III.A or B
	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?	III.C.3
	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	III.C.2

Use Manual to Gather Background Information

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

- 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



Four Steps – Checklist

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 (more than 20 samples)

- 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



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 ID Theft Victims

FTC's Complaint Database

Identity Theft Data Clearinghouse

- Federal government's centralized database of identity theft victim complaints
 - Available for **FREE** through the Consumer Sentinel Network (CSN)
 - Over 1.8 million searchable complaints
 - Register at <http://register.consumersentinel.gov>



Consumer Educational Materials

- Take Charge: Fighting Back Against Identity Theft
- AVOID ID Theft: Deter, Detect, Defend



www.ftc.gov/bulkorder

Training Materials: Deter, Detect, Defend Education Kits

**TALKING ABOUT IDENTITY THEFT:
A HOW-TO GUIDE**



DETER · DETECT · DEFEND

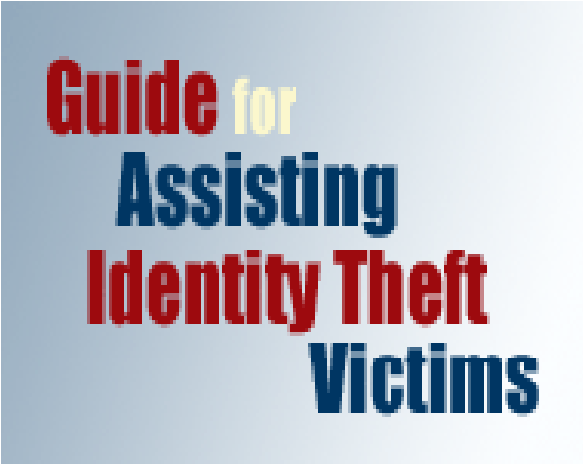
AVOID THEFT

www.ftc.gov/idtheft



Additional Resources

- **Guide for Assisting Identity Theft Victims**
<http://www.idtheft.gov/probono/>
- Identity Theft Microsite
<http://www.idtheft.gov>



Guide for
Assisting
Identity Theft
Victims



Additional Resources

- Privacy Rights Clearinghouse, www.privacyrights.org
- National Center for Victims of Crime, (202) 467-8700, www.ncvc.org
- National Crime Victim Law Institute, www.ncvli.org/ and the Responding to Online Fraud Project contact
 - Meg Garvin (garvin@lclark.edu ~ 503-768-6953)
 - Johanna Borkan (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/>



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

Interactive Training

Victim Assistance Training Online (VAT *Online*)

www.ovcttac.gov/vatonline

- web-based training program for individuals that offer assistance to victims of crime



Victim Assistance Training *Online*
New Web-Based Training Program for
Victim Service Providers

The Office for Victims of Crime (OVC) is pleased to announce a new online training opportunity for victim service providers. Victim Assistance Training Online (VAT *Online*) provides professionals with the basic skills they need to assist victims effectively and sensitively.

Learn anytime, anywhere. With the click of a mouse, service providers can access foundation-level training 24/7 from any Internet-accessible location.

No costs attached. The course is available free of charge . . . no tuition fees, no travel expenses!

Learn at your own pace. VAT *Online* is divided into sections that can be completed when convenient. The total course time is approximately 35-40 hours. Just bookmark your place and start where you left off.

Learn something new . . . or refresh your learning. VAT *Online* is for victim service providers with less than 3 years of experience. It is also useful as a refresher course for seasoned professionals.

Stay abreast of emerging issues. The course will be updated every 2 years to make sure the content is current and relevant.

Maximize your training dollars. VAT *Online* provides supervisors with the opportunity to ensure that their staff has access to high-quality training whenever needed.

COMPUTER REQUIREMENTS
VAT *Online* can be used with either a Mac or PC. Hardware and software requirements include—

- Windows 95, 98, 2000, NT, ME, or higher
- Mac OS 9 or OS X or higher
- 64 mb RAM
- 56K modem minimum speed
- Microsoft Word, Adobe Acrobat Reader
- Macromedia Flash Player
- Screen resolution best at 1024 x 768

VAT *Online* available at
www.ovcttac.gov/vatonline

To learn about other training opportunities available from the Office for Victims of Crime, contact OVC's Training and Technical Assistance Center at
www.ovcttac.gov

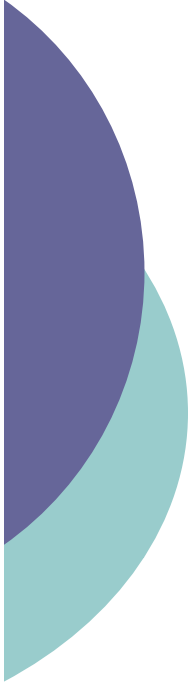
VAT *Online* is funded by the U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime. The training was developed by Crestall Associates, Inc., in partnership with the National Center for Victims of Crime and Safe Horizon, Inc.

OVC **OVCTTAC**
Office for Victims of Crime
Training and Technical Assistance Center

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

Deanya Kueckelhan

214-979-9350

dkueckelhan@ftc.gov