

Federal Trade Commission DOJ-Access to Justice Initiative



**Webinar for the
Legal Service
Community**

July 10, 2013

Welcome

Sylvia Dominguez-Reese, Access to Justice



- Who we are
- The FTC's Legal Services Collaboration
- Identity theft presentation
- Consumer education resources
- Questions and answers

Federal Trade Commission

Carol Kando-Pineda, FTC



- What is the FTC?
 - Independent law enforcement agency with civil authority
 - Broad jurisdiction: Unfair deceptive acts or practices
 - Investigations/litigation
 - Consumer and Business Education

Legal Services Collaboration

Monica Vaca, FTC



- Sharing expertise
- Case referrals: *e.g., FTC v. Freedom Companies (mortgage assistance scam)*
- Engaging in other forms of advocacy: *e.g., amicus briefs*
- Consumer education: *e.g., consumer.gov*

Consumer Education



- All materials are free, in the public domain, and can be bulk ordered.
- Most in English and/or Spanish.
- On most issues, we have levels of information:
 - Bookmarks: for people who need just the high points
 - Consumer alerts: with a little more information
 - Facts for consumers: with a lot of information
- Examples: Guides to Purchasing a Used Car or a Funeral, ProBono Guide about Identity Theft

FTC Contacts



Northwest Region in Seattle:
Julie Mayer jmayer@ftc.gov

Northeast Region in
New York:
Robin Eichen
reichen@ftc.gov

Western Region in San Francisco:
Laura Fremont lfremont@ftc.gov

Midwest Region in Chicago:
Joannie Wei jwei@ftc.gov

Join the FTC's Legal
Services Listserv -- email
tthomas@ftc.gov

Western Region in Los
Angeles: Faye Chen Barnouw
fbarnouw@ftc.gov

East Central Region in Cleveland:
Maria DelMonaco
mdelmonaco@ftc.gov

Southwest Region in Dallas:
Emily Robinson
erobinson@ftc.gov

Southeast Region in Atlanta:
Barbara Bolton bbolton@ftc.gov

Identity Theft: What We Will Cover

Lisa Schifferle, FTC



- Overview: Understanding Identity Theft
- Assisting Victims of ID Theft
 - Financial Account ID Theft
 - Non-Financial ID Theft
 - Child ID Theft
- Case Study: Using the *Guide for Assisting Identity Theft 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.

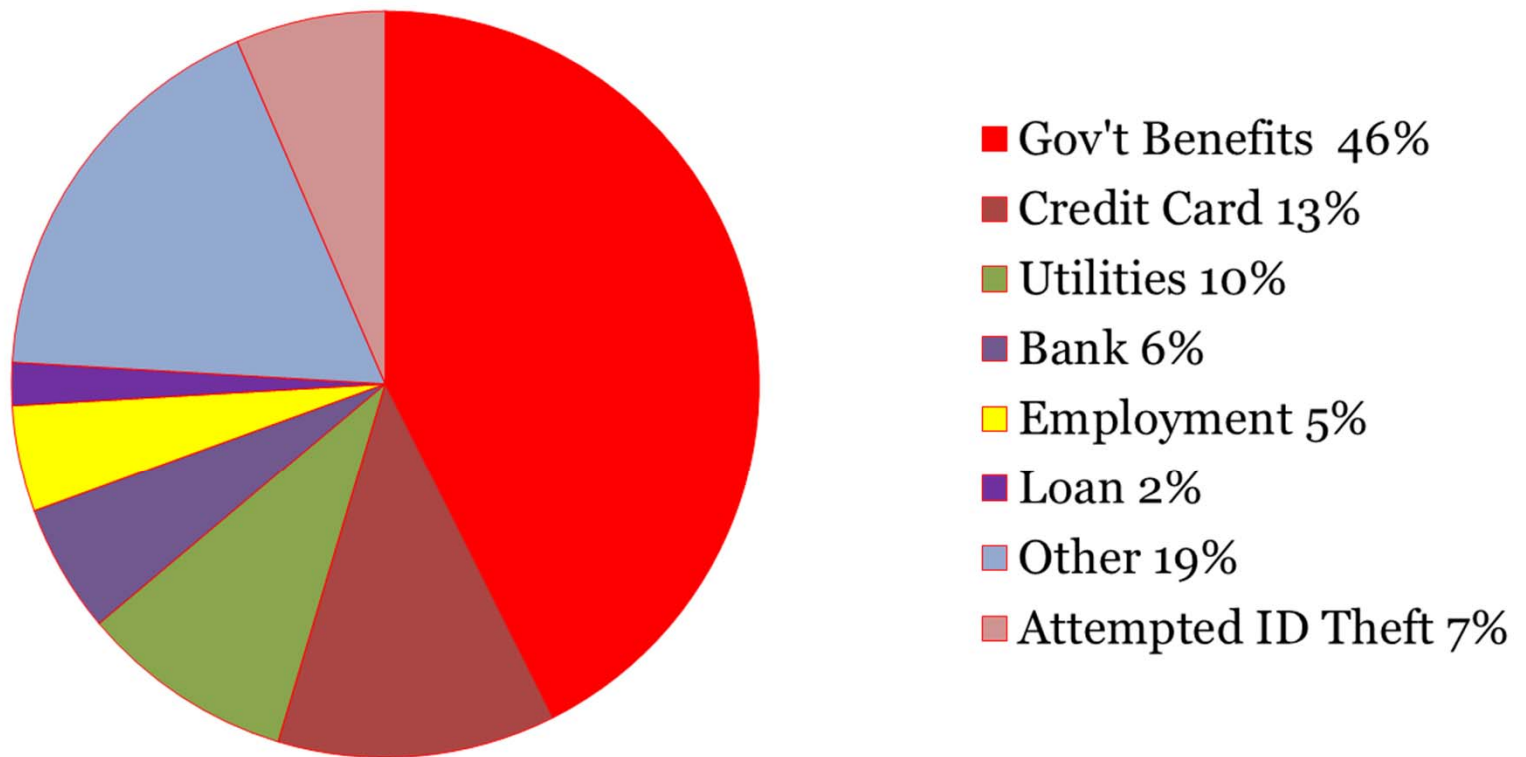
Scope of ID Theft Problem




- 9 million new victims annually
- #1 complaint to Consumer Sentinel in 2012
- 18% Sentinel complaints were identity theft in 2012

How Victims' Information is Misused

Government Benefits is most common form of ID Theft



The Impact of ID Theft

- 
- Denial of credit
 - Loss of credit rating
 - Harassment by bill collectors
 - Lawsuit
 - Garnishment
 - Time and expense
- Tax problems
 - Arrest
 - Denial of driver's license renewal
 - Loss/denial of employment
 - Denial of public benefits
 - Denial of medical care

The Emotional Impact of Identity Theft



- Victims may experience:
 - embarrassment
 - sadness
 - helplessness
 - anger
 - isolation
 - betrayal
 - rage
 - suicidal feelings

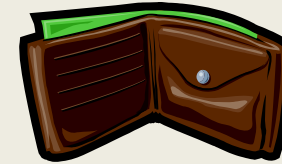


HOW DOES IDENTITY THEFT HAPPEN?

Old-fashioned identity theft



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



New, high-tech identity theft



- Skimming
- Data breaches
- Phishing

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.





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

Data breach example: TJX Cos.



- TJX allegedly:
 - Stored or transmitted consumer information in clear text when on computers in TJX's stores
 - Stored information for up to 30 days, when no longer needed
 - Used commonly known default user IDs and passwords to protect their files
 - Failed to use readily available security measures to prevent unauthorized wireless connection to its networks
 - Failed to use measures sufficient to detect unauthorized access

TJX gets 20 years of FTC scrutiny for security failures

By [Layer 8](#) on Thu, 03/27/08 - 10:20pm.

Share Tweet This Email this page Comment Print

Newsletter Sign-Up

Discount retail giant TJX today settled [Federal Trade Commission](#) charges that it failed to provide reasonable and appropriate security for sensitive consumer information.

The [settlement](#) requires that the company implement comprehensive information security programs and obtain audits by independent third-party security professionals every other year for 20 years. No fines or consumer reimbursements were part of the settlement.

[TJX](#) revealed last year that it had suffered a massive computer network security failure over a period of years that exposed over 100 million credit cards. The FTC settlement doesn't get the company [out of the woods](#) however as almost 40 [states](#) and other Federal investigations loom.

According to the FTC complaint, [TJX, with over 2,500 stores worldwide](#), failed to use [reasonable](#) and appropriate security measures to prevent unauthorized access to personal information on its computer networks. An intruder exploited these failures and obtained tens of millions of credit and debit payment cards that consumers used at TJX's stores, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. Banks have claimed that tens of millions of dollars in fraudulent charges have been made on the cards and millions of cards have been cancelled and reissued.

Specifically, the agency charged that TJX:

- * Created an unnecessary risk to personal information by storing it on, and transmitting it between and within, its various computer networks in clear text;
- * Did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to its networks without authorization;
- * Did not require network administrators and others to use strong passwords or to use different passwords to access different programs, computers, and networks;

Advertisement:

About Layer 8

Layer 8 is Network World's daily home for the not-just-networking news.

[RSS](#) [Contact Requires Login](#)

Archives

June 2009
May 2009
April 2009
March 2009
February 2009
January 2009

Categories

Ares
Bill Gates
CIA
Communications
DARPA
Data Center

Phishing



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

Example



- 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.

Victims may need a lawyer when:



- their age, health, language proficiency, or economic situation affect self-representation
- they are sued or harassed by creditors attempting to collect debts incurred by an impostor
- creditors or credit reporting agencies are uncooperative
- they need help with their rights when their identity thief is arrested
- their case is complex or involves non-financial identity theft



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 – it will generate an “ID Theft Affidavit” for victim’s use
4. File a Police Report – combined with the ID Theft Affidavit, is an “Identity Theft Report”

1. Contact CRAs



- Place Fraud Alerts on Credit Reports
- Consider Credit Freeze
 - Prohibits CRAs from releasing the consumer's credit reports or credit scores without consumer's authorization
- Obtain Credit Report *free of charge*

Fraud Alert vs. Credit Freeze



Fraud Alert

- One call
- Creditors must take “reasonable steps” to verify identity
- Less effective
- 90 days (renewable) or 7 years

Credit Freeze

- Write each bureau
- No one can apply for new credit – must thaw the report
- More effective
- Effective until thawed
- Possible fees

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 its actions

Request Business Records Related to Theft (FCRA 609e)



- Victim is entitled to copies of transaction records related to theft of identity, such as applications for credit
- Victim can also authorize law enforcement to receive records directly, without need for subpoena

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:
 - ftc.gov/idtheft
 - 877-438-4338
 - TTY: 866-653-4261
 - or by mail
- ID Theft Complaints will generate and populate an “ID Theft Affidavit” for victim’s use
- The FTC does not take enforcement actions on behalf of individuals

4. File a Police Report



- Call the local police as soon as possible
 - Request a copy of official police report/Identity Theft Report
- Some state laws require police to write reports for identity theft victims
 - A map of 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 right under FCRA § 605B
 - Permanently removes the identity theft-related information from credit reports
- 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
 - notify furnishers that information it furnished resulted from identity theft

Credit Reporting Agencies' Dispute Obligations – FCRA §611



- **When a customer notifies CRA of a dispute:**
 - CRA must send dispute to furnisher of disputed information
 - Furnisher must investigate dispute and report back to CRA within 30 days
 - CRA must notify consumer of results of investigation
 - If no corrections to credit report, consumer has a right to include a dispute statement
 - ✦ 100 words, but CRA can replace with a dispute number

Victims May Need a Lawyer to Assert Rights Under Federal Civil Laws



- Fair Credit Reporting Act (FCRA)
- Fair Credit Billing Act (FCBA)
- Electronic Fund Transfer Act (EFTA)
- Fair Debt Collections Practices Act (FDCPA)



ASSISTING VICTIMS OF NON-FINANCIAL IDENTITY THEFT

Medical Identity Theft



- Occurs 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
- May be difficult to remedy because of HIPAA concerns

How to Assist Victims



- Report theft to local law enforcement and get a copy of report.
- 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 thief.
Important: Do not mention identity theft at this point.
- Review records and write providers who gave care to their requesting correction or segregation and flagging of records.
- Confirm that records have been corrected.

Tax & Employment Identity Theft



- Use of victim's personal identifying information to obtain or retain employment
- Usually discovered through IRS notice or denial of public benefits

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:
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 CRAs if the account appears on victim's credit report
 - Send dispute letter and request for business records to utility provide



ASSISTING CHILD IDENTITY THEFT VICTIMS

How big a problem is child ID theft?



- Carnegie Mellon CyLab Study:

<http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf>

- Study looked at 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

Why are children vulnerable to ID theft?



- Clean credit is appealing to identity thieves
- Information readily available in many contexts
- Theft of child identity can go undetected for long periods of time

Special Tips for Monitoring a Child's Credit



- Children should not have active credit files with CRAs
- No need to check every year unless child's info is at risk
- Helpful to order credit report close to child's 16th birthday, so can clear up errors before child needs credit
- Ask for “manual search.” Do not use annualcreditreport.com for children.

Special Tips for Monitoring a Child's Credit



- Explain that child is a minor (under age 18) who cannot legally enter into any contract
- Provide Uniform Minor's Status Declaration and/or birth certificate
- Ask CRA to immediately remove all accounts, application inquiries and collection notices from child's file

Special Tips for Monitoring a Child's Credit



- Explain that child is a minor (under age 18) who cannot legally enter into any contract
- Provide Uniform Minor's Status Declaration and/or birth certificate
- Ask CRA to immediately remove all accounts, application inquiries and collection notices from child's file

Victims in Foster Care



- More susceptible
- Harder to remedy
- Consequences may be more severe

Child and Family Services Improvement and Innovation Act of 2011



- Provides that child welfare agencies must determine whether foster children, ages 16 and older, have a credit file
- Requires the child welfare agencies to resolve any inaccuracies in the credit reports
- Obligation continues until child is emancipated from foster care
- Signed in to law in late September 2011



**CASE STUDY:
USING THE *GUIDE FOR
ASSISTING IDENTITY
THEFT VICTIMS***

Case Study: “Jane Doe”



- Jane’s birth certificate and Social Security card are stolen
- Thief takes job, pays taxes, opens credit cards, and has baby using Jane’s name
- Employment, tax, financial & medical identity theft
- How do you use the *Guide* to help your client, Jane?
- (Note: this case study is based on a true story!)

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 *Guide* 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](#)

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



- FCRA 605B Blocking Request Letters
- FCRA 611 and 623 Dispute Letters
- Letters disputing fraudulent charges
- FCRA 609(e) Letters requesting business records
- Letters concerning rights under FCBA, EFTA, FDCPA
- Consumer & Attorney letters

Everything in one place



- *Guide* has copies of all statutes relevant to the rights of identity theft victims (or portions thereof), including:
 - FCRA & FACTA Amendments
 - FDCPA
 - Fair Credit Billing Act
 - Electronic Funds Transfer Act
 - Dept. of Education regulations

Online Materials for ID Theft Victims



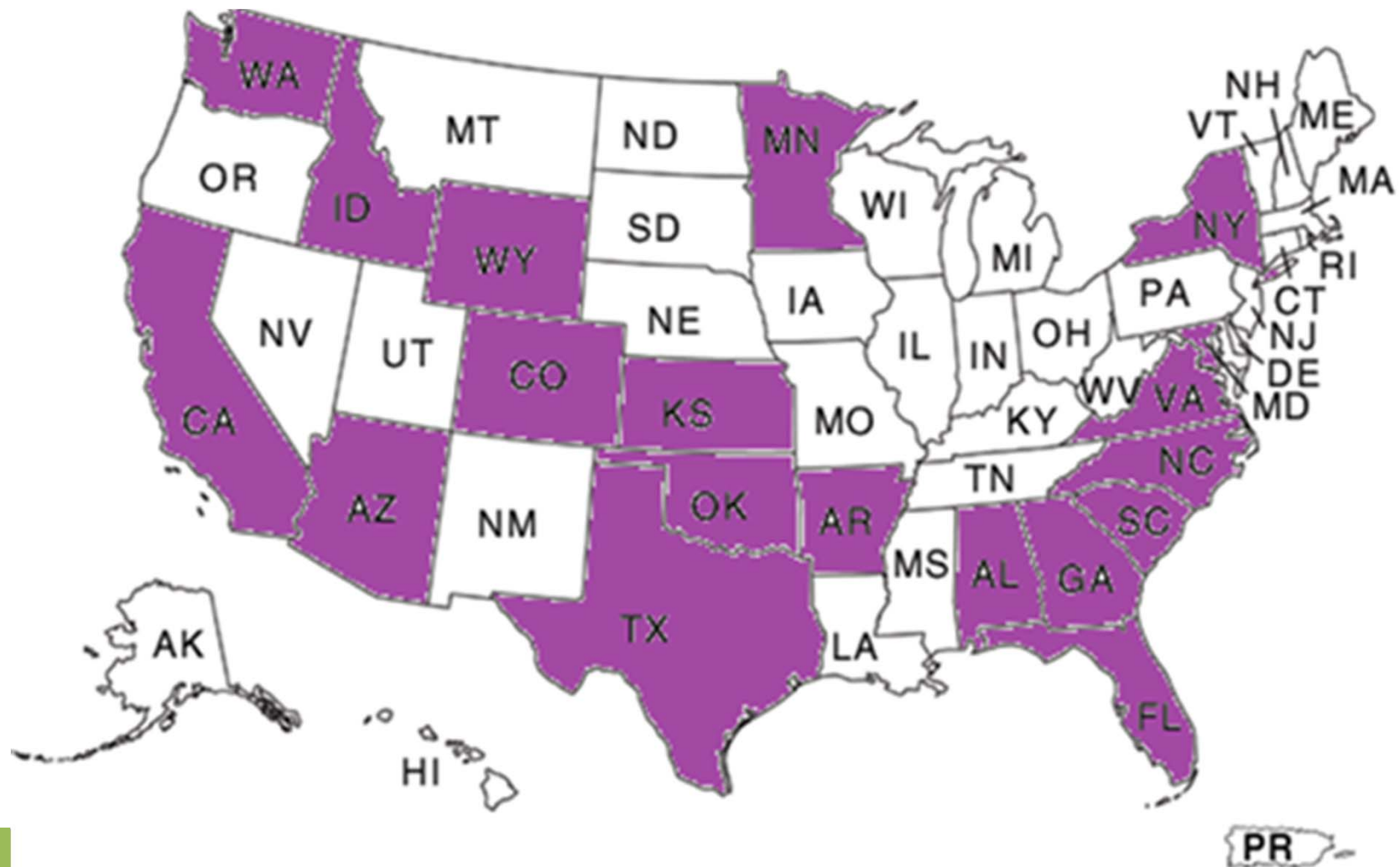
- NITVAN = National Identity Theft Victim Assistance Network
 - Network of 10 coalitions builds field's capacity to address IDT victims' rights & needs
- NITVAN along with partners at Kansas Legal Services & Probono.net created & launched online Access to Justice (A2J) assistance package for victims of IDT.
 - Automated creation of letters – mirroring those created by FTC for pro bono attorneys to help victims
 - Info about options, links to helpful resources also included
 - Spanish forms may be coming in the future

What self-help forms were created?



- **Letter to Creditor** – to creditor about bill as a result of IDT.
- **Letter to Debt Collector** – respond to company or law firm that is a debt collector, or collecting a bill victim did not authorize.
- **Letter to Credit Bureau** - create a letter to credit bureau, seeking investigation & removal of items resulting from IDT.

IdentityTheftNetwork.org/GetHelp





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.

Resources For You

Carol Kando-Pineda, FTC



CONSUMER.GOV



Consumer.gov

Reaching legal services
audience

- **Reaching new audiences**
 - Different needs
 - New educational approach
- **Input on issues, approach, audience from:**
 - Legal services
 - Non-profits
 - Teachers, especially TESOL teachers



Consumer.gov

- **Training in:**
 - Rethinking the message
 - Writing
 - Design
- **Question:**
 - Not what we need to say, but what the audience needs to know.
- **Aimed at:**
 - People who want just the consumer protection basics plain and simple.

Consumer.gov

- Different audience
- Website
- Print
- Read-along audio
- Simplified video
- Resources for community leaders

consumer.gov
what to know and do

 search

Español

Managing Your
Money



Credit, Loans
and Debt



Scams and
Identity Theft



Help for You

Consumer protection basics... plain and simple.





Consumer.gov

Each topic includes:

What it is

What to know

What to do

- **What It Covers**

- Managing your money
- Credit, loans and debt
- Scams and identity theft
- Help for you
 - ✦ Presentations
 - ✦ Handouts
 - ✦ Worksheets
 - ✦ Videos
 - ✦ Links to more information. Please let us know if you have resources we can link to!



Consumer.gov

- **How can you use these resources?**
 - Link to it
 - Use the text in your site, newsletters
 - Adapt the text to your needs
 - Print and distribute “What to do” and worksheets
 - Use sample presentations or worksheets
 - Grab videos/graphics for your own website
 - Order free printed materials



Consumer.gov

consumer.gov
what to know and do



visit bulkorder.ftc.gov for free materials

Contact Information

Lisa Schifferle, FTC

202-326-3377

lschifferle@ftc.gov

Carol Kando-Pineda, FTC

ckando@ftc.gov

Silvia Dominguez-Reese

U.S. Department of Justice-Access to Justice Initiative

Silvia.Dominguez-Reese2@usdoj.gov