# IDENTITY THEFT:

## *Is Your Bank Account Hack Proof?*

March 30, 2015

**To find out more about the Washington Coalition of Crime Victim Advocates:**

**www.wccva.org**

**(360) 456-3858**

**To find out more about the national network of Coalitions, visit:**

**www.identitytheftnetwork.org**

Part I

# The Impact of Identity Theft and Fraud

# Consumer Sentinel Network Complaint Figures

*January 1 - December 31, 2014*

## Total Number of Identity Theft, Fraud and Other Consumer Complaints = 47,057

### Fraud and Other Complaints Count from Washington Consumers = 36,127

*Top 10 Fraud and Other Complaint Categories Reported by Washington Consumers*

| Rank | Top Categories | Complaints | Percentage[1] |
|---|---|---|---|
| 1 | Impostor Scams | 5,542 | 15% |
| 2 | Debt Collection | 3,249 | 9% |
| 3 | Banks and Lenders | 2,629 | 7% |
| 4 | Telephone and Mobile Services | 2,115 | 6% |
| 5 | Auto-Related Complaints | 1,474 | 4% |
| 6 | Prizes, Sweepstakes and Lotteries | 1,362 | 4% |
| 7 | Shop-at-Home and Catalog Sales | 1,259 | 3% |
| 8 | Television and Electronic Media | 1,171 | 3% |
| 9 | Internet Services | 1,077 | 3% |
| 10 | Health Care | 841 | 2% |

[1]Percentages are based on the total number of CSN fraud and other complaints from Washington consumers (36,127).

Note: These figures exclude complaints provided by the Washington Office of Attorney General.

# Identity Theft Complaints Count from Washington Victims = 10,930

## *Identity Theft Types Reported by Washington Victims*

| Rank | Identity Theft Type | Complaints | Percentage[1] |
|---|---|---|---|
| 1 | Government Documents or Benefits Fraud | 6,050 | 55% |
| 2 | Credit Card Fraud | 1,243 | 11% |
| 3 | Phone or Utilities Fraud | 667 | 6% |
| 4 | Bank Fraud | 619 | 6% |
| 5 | Employment-Related Fraud | 339 | 3% |
| 6 | Loan Fraud | 145 | 1% |
| | Other | 2,724 | 25% |
| | Attempted Identity Theft | 411 | 4% |

[1]Percentages are based on the 10,930 victims reporting from Washington. Note that CSN identity theft complaints may be coded under multiple theft types.

# 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.

# Easy Access

Card electronic strip readers


Cameras to view password entry

Keystroke Capturers

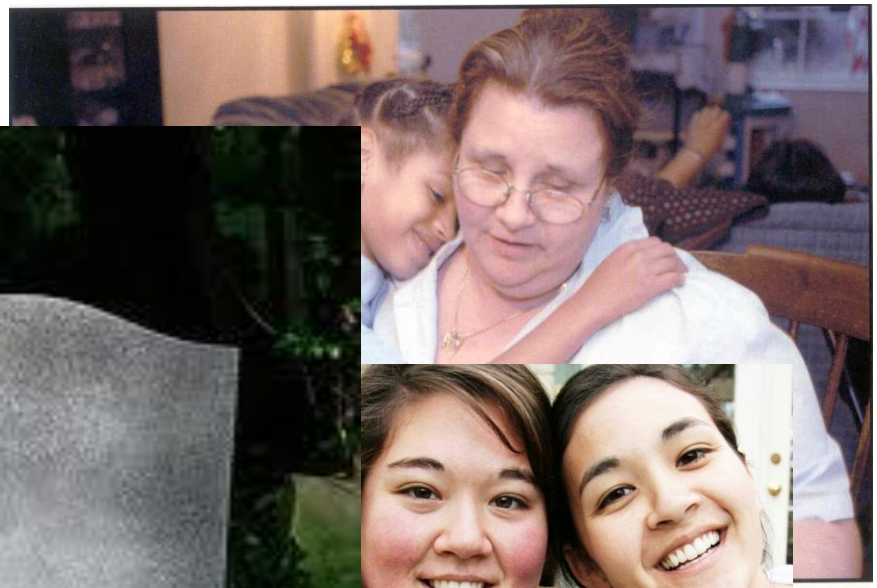
# Non-Financial Identity Theft

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

# Targeted Populations

- Elderly
- Homeless
- Battered Women
- Children
- Military
  - In August 2013, Washington State had one of the largest military populations in the United States, with over 64,000 active duty military personnel

# Who Can Be A Victim?



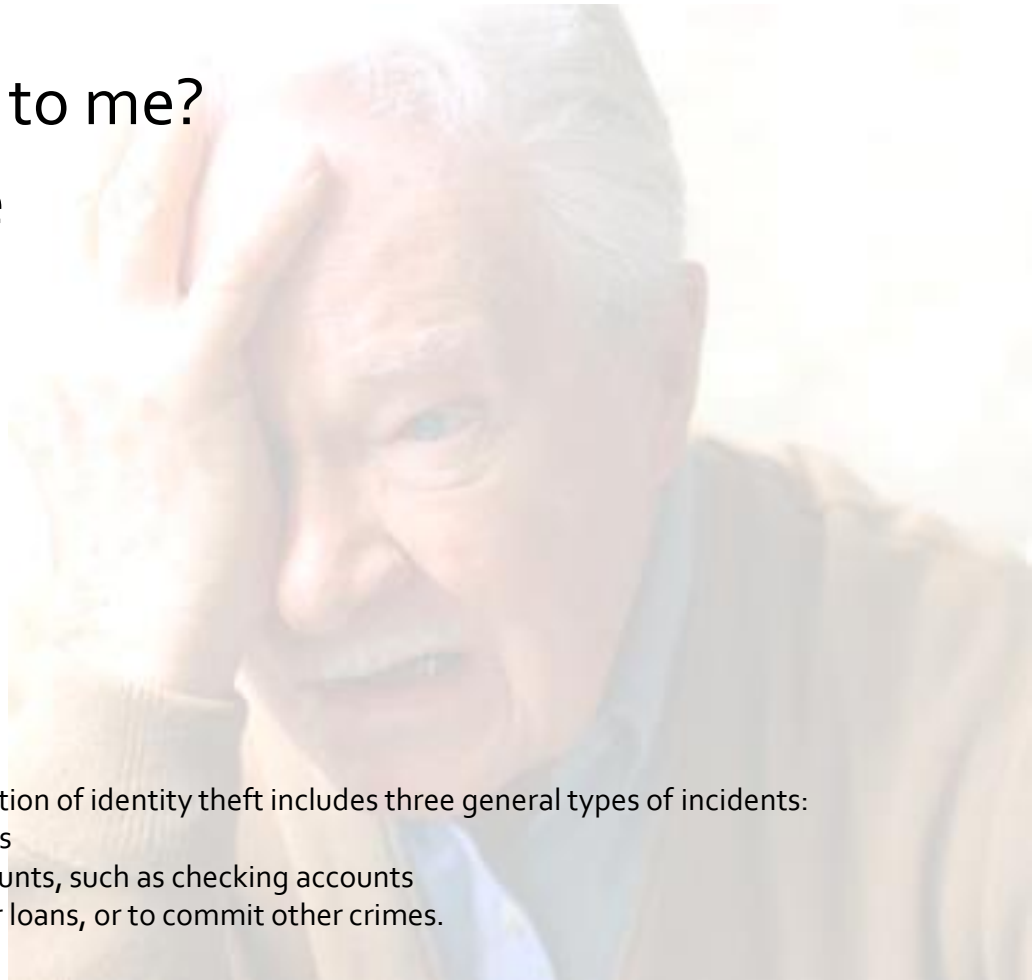
# Consequences of Identity Theft:

1. Denial of credit
2. Increased rates and financial charges
3. Loss of employment
4. Inability to get a job
5. Bankruptcy
6. Arrest
7. Loss of money associated with repairs
8. Missed opportunities (housing, employment, education)

# How Does Identity Theft Affect Victims?

53% of 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



For the National Crime Victimization Survey (NCVS), the definition of identity theft includes three general types of incidents:

- unauthorized use or attempted use of existing credit cards
- unauthorized use or attempted use of other existing accounts, such as checking accounts
- misuse of personal information to obtain new accounts or loans, or to commit other crimes.

# FINANCIAL FRAUD in THE UNITED STATES

## The Non-Traditional Costs of Financial Fraud

**$50 BILLION per year is lost to fraud...but that's not the whole story.**

There is an **emotional side of fraud** that is not often talked about.

NEARLY **2/3** of victims reported experiencing at least one non-financial cost of fraud to a serious degree.


Beyond emotional costs, nearly half of fraud victims reported **incurring indirect financial costs** associated with fraud.

**25%** paid late fees

**23%** paid fees for bounced checks

**9%** reported declaring bankruptcy

**29%** of victims who incurred indirect costs **paid more than $1,000**

Almost half of the victims **blame themselves** for being defrauded. But there are ways you can protect yourself and **avoid becoming a financial fraud victim**.

Visit SaveAndInvest.org/FraudCenter
to learn more about fraud–and how to spot and avoid it.

Source: FINRA Investor Education Foundation research report, *Non-Traditional Costs of Financial Fraud* (2015). Study and methodology available online at SaveAndInvest.org.

SaveAndInvest.org

Part II

# But, How Do You Stay Safe…?

# …*Really?*

# Pop Quiz!

- What is the 100% thief/fool-proof, guaranteed way to hack proof your account and never, *ever* become a victim of identity theft or fraud?
  - *If you find out, would you let the rest of us know?*

- **But, making the following tips your *Banking Basics* will make it tougher for thieves to steal from consumers!**

# Basics for Banking: Safety Tip #1

- Would you leave your wallet sitting on a table, unattended in a busy restaurant, in an unknown city, while you walked away?
  - **If you said 'No'… then you probably don't want to leave your finances open for the world on unsecured Wi-Fi.**
    - *Unprotected banking = No Go!*

# Basics for Banking: Safety Tip #2

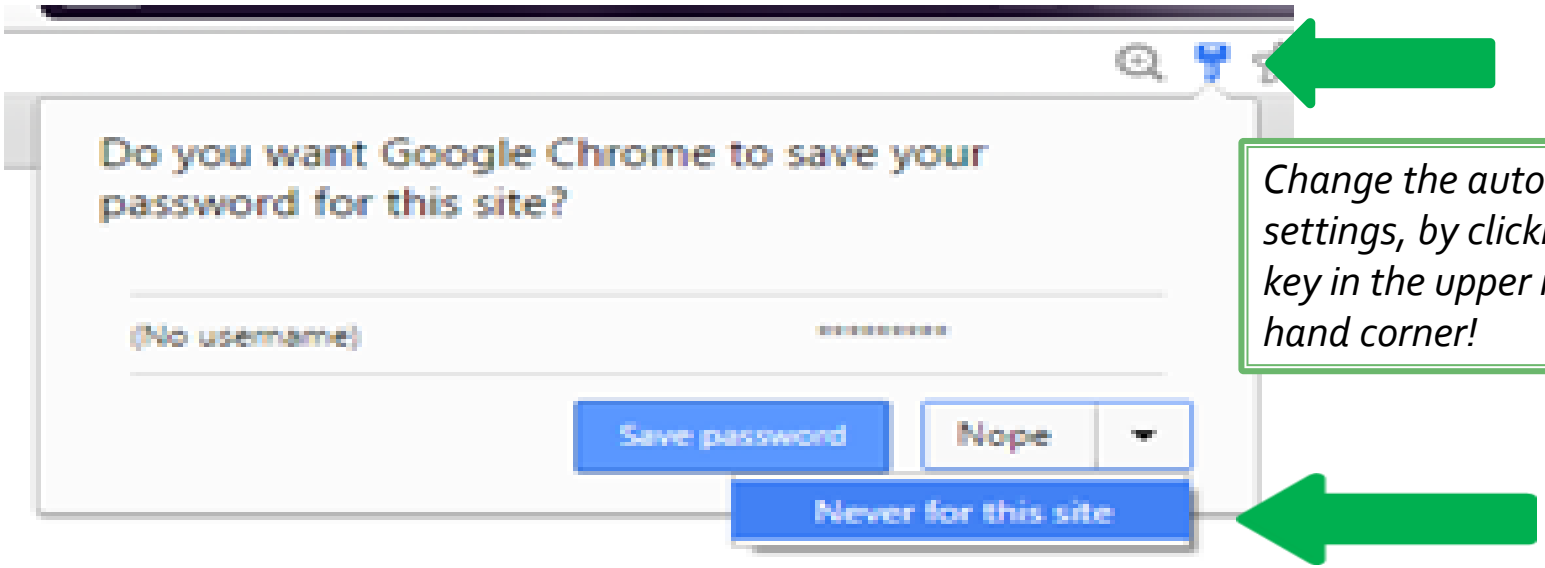
- **Make passwords part of your banking Standard Operating Procedures (SOP)**
- Everything that can have a password, should!
- When it comes to passwords, variety is the spice of life! Change them up and change frequently!
- Password protect: home screens, your phone, tablet, iPod, computer… *If you lose it: thieves **will** try to get in it!*
- Set *all* devices to automatically lock/secure!

# Basics for Banking: Safety Tip #3

- **Who Contacted Who, First?**
- **Did you contact your bank, first?**
  - YES: Great! Makes sense!
  - No? Hit the brakes!
- **Why is the Bank Calling You?**
  - Duh! Of course, I expected this call! I've been luxuriously traveling throughout Europe after winning the lottery!
  - Odd… I have NO idea!
- **Why is the bank asking such sensitive questions?**
  - *They shouldn't be!*
  - It is 100% okay to hang up or end contact with any one, any time.

# Basics for Banking: Safety Tip #4

- **Just say no…** to "auto-save" or "stay logged in?" or "auto-fill"
  - *It may save 30 seconds - 1 minute out of your day, but it could cost much more in the long-run!*




*Change the auto-save settings, by clicking on this key in the upper right hand corner!*

# Basics for Banking: Safety Tip #5

- **If You Don't Need It, Don't Keep it!**
- **Fraud Alert Texts from 1 week or 6 Months Ago?**
  - Don't need: Delete!
- **Bizarre Text Message From Unidentified Number?**
  - Definitely Don't Need! Also, don't open: just delete!
  - If it's someone who *actually* knows you: they will find you
- **Texts That Have Personal Information In Them?**
  - Not that any of us have ever done that… but… just delete!

# Basics for Banking: Safety Tip #6

- **Treat a lost device like a lost or stolen credit or debit card**
  - Report that it has been lost or stolen to your phone provider and banking institution.
    - Most banks and credit unions are great about helping you through this!
    - Phone providers can pause or freeze phone service, so it can't be used.

***And, then pause to smile about how smart you were to password protect everything you could!***

# Basics for Banking: Safety Tip #7

- **Hello, is it *the app* you're looking for?**
  - It may look, sound or appear like a trusted app or your bank… but, is it really?
  - Go to your bank or CU's website, or visit a branch, and find the specifics of their app!

# Banking Safety Tips Recap

1. Only use secured internet for banking.
2. Always use passwords and "code words"
3. If you didn't initiate contact, or the questions are fishy (or, "phishy") – end contact
4. Skip auto-save. You don't need it.
5. Delete old texts, fraud alerts or sensitive information
6. Report and secure lost devices, ASAP
7. Double check authenticity of apps

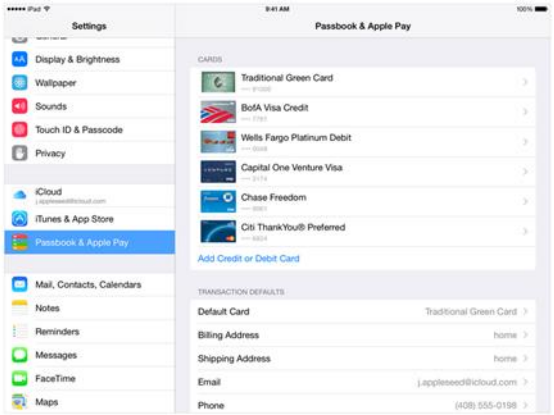
## Part III

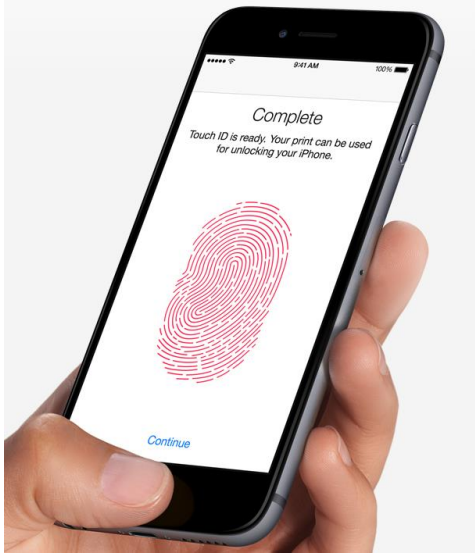
# Online Pay Services

# Online Pay Services

- **Apple Pay**
- **"Apple Pay offers an easy, secure, and private way to pay using Touch ID on iPhone 6, iPhone 6 Plus, iPad Air 2, and iPad mini 3."**
- "You can use Apple Pay with your iPhone 6 and iPhone 6 Plus to pay in stores that accept contactless payments."
- "On iPhone 6, iPhone 6 Plus, iPad Air 2, and iPad mini 3, you can use Apple Pay to pay within apps when you see the "Buy with Apple Pay" or "Apple Pay" button as a payment method."

***Apple, Inc (2015): [https://support.apple.com/en-us/HT201469](https://support.apple.com/en-us/HT201469)***

# Online Pay Services

- **Google Wallet**
- **"Google Wallet is a free digital wallet that securely stores your credit cards, debit cards, gift cards, loyalty cards, offers, and more. With Google Wallet, you can shop in stores, buy online, and send money.**
- Stores gift cards, loyalty cards and offers on the Google Wallet app. You can also purchase in stores using the Google Wallet Card
- You can use Google Wallet to buy on Google Play or other Google products, and on select Android apps and sites, wherever you see the Buy with Google button.
- You can send or request money to anyone in the U.S. with an email account through Gmail or the Google Wallet app. If they don't have a Google Wallet already, they can create one in order to send and receive money.
- In addition, you can track your online purchases, get shipping notifications, and view detailed order history using the Google Wallet app."

# Online Pay Services

- **But, are online pay services *safer*?**
- Not an entirely new concept… Apple Pay was released in the Fall of 2014 and Google Wallet released in 2011. Other online pay services, like PayPal, having been around since early 2000's.
- BENEFITS*:
  - No "swipe"
  - Considered "harder to hack"
  - Current credit card storage systems have shown big vulnerabilities (For example, Target and Home Depot breaches)
  - Ease of use, easy set-up, especially Apple
  - Setup requires approval by banks; for example, WSECU plans to add Apple Pay in the near future.
  - Banking information isn't displayed, or easy to find/see, etc.

The Washington Post: *Apple Pay's pitch: Simpler is better. But some security experts disagree.* (March 23, 2015)

# Online Pay Services

- **But, are online pay services *riskier*?**
- Not an entirely new concept… Apple Pay was released in the Fall of 2014 and Google Wallet released in 2011. Other online pay services, like PayPal, having been around since early 2000's.
- AREAS OF CONCERN*:
  - Not widely used/implemented, yet, so consumers are still carrying credit cards.
  - Easy to use and easy to set-up, even with stolen credit card information.
  - Concerns over weeding out "good/safe" consumers from unsafe ones. Ie: is the approval process for Apple Pay "good enough"?
  - Who maintains liability for fraudulent purchases? Apple? Banks? Merchants?
  - An estimated 96% of all apps have an identified security weakness…

*The Washington Post: *Apple Pay's pitch: Simpler is better. But some security experts disagree.* (March 23, 2015)

# A Final Thought About Banking Safety

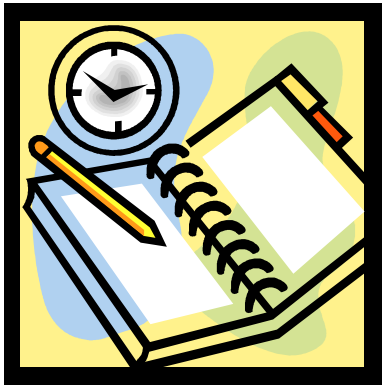
- Hackers and identity thieves ***FULL-TIME JOB*** is to steal and find new ways to exploit others, for their personal gain and profit.
- It's okay to let others test drive new technologic developments.
- Do what ***you can*** to make thieves "work" harder!

# Part IV

# The Recovery:
## After Theft Occurs

# Initial Steps

- First Contact
- Maintaining a Log
  - "Chart Your Course of Action"
  - Helpful Documents
    - Government-issued IDs
    - Utility bills or other monthly statements showing victim's address
    - One or more credit reports showing fraudulent activity
    - Collection letters, credit card or bank statements, or any cards or merchandise received but not ordered
    - A log showing actions victim may have taken to date



# Step 1: Contact Companies where Thief Committed Fraud

**Advise victim to:**

- Contact fraud dept. - not customer service
- Instruct company to immediately close or freeze accounts fraudulently opened/used
- Send written dispute including ID Theft Affidavit – police report should *not* be required
- Request closure letter from company describing results of their actions
- Request ID theft-related documents
- Ask where to send dispute & document request

# Step 2: Contacting CRAs

Placing an Initial **Fraud Alerts** on Credit Reports

- Signals potential creditors that someone else is using consumer's identity
- Only have to contact one of the 3 CRAs
- Last 90 Days
- Creditor *must* take additional steps to confirm the applicant's identity before issuing new credit, raising limit, etc.
- Entitles victim to free credit report when requested

# Step 3:
# File a Complaint with the FTC

- FTC hotline phone counselors & web-based consumer guidance to help victims recover
- File an ID Theft Complaint with FTC:

  www.ftc.gov/idtheft

  877-438-4338 or TTY: 866-653-4261
- Filing with FTC does not substitute for a report to criminal law enforcement. FTC does not take enforcement actions on behalf of individuals.

***Remember: Victims need ID Theft Report for Blocking Info = FTC ID Theft Complaint + Police Report***

# Step 4:
# File a Police Report

1. Request an appointment for in-person report filing
2. Take along completed FTC ID Theft Complaint
3. Request copy of Official Police Report***:*** Officer may attach ID Theft Affidavit to police report, or department's own police report's details may suffice the goal is to get an ***Identity Theft Report***

# Monitoring Credit Reports

Look for:

1. Accounts victim didn't open
2. Activity on accounts victim had closed or were dormant
3. Changes to personal info such as name, address, DOB, SSN, employer
4. Credit inquiries from companies victim didn't contact

# Disputing Fraudulent ATM & Debit Card Transactions

- Educate consumers about these short timeframes
- Electronic Fund Transfer Act (EFTA) & Regulation E, issued by the Board of Governors of Federal Reserve, sets forth 3 tiers of liability for unauthorized ATM or debit card uses:

1. If victim reports lost/stolen card within 2 business days after discovering
2. If victim fails to report within 2 business days after discovery, but does report its loss within 60 days after statement is mailed
3. If victim fails to report an unauthorized transfer within 60 days after their statement is mailed

# Credit Card Issuer Obligations under the FCBA

Fair Credit Billing Act, *15 U.S.C. § 1601*, (FCBA)

Limits liability to a max of $50 per card. Victim must:

- send <u>timely</u> certified mail notice of error to creditor
- include name, address, account #, description of billing error, including amount & date of error
- ensure letter reaches creditor within 60 days after first bill containing error was mailed.

# Obtaining Business Records Relating to Identity Theft

Victims are entitled to copies of records relating to the theft of their ID, such as applications for credit, under section 609(e) of the Fair Credit Reporting Act:

- Business must give victim copies of applications & other business records resulting from theft.
- Within 30 days, at no cost, without subpoena.
- All requests must be in writing.
- Business may specify an address to receive these requests. Victim should ask business to verify address to which to send request.

# Long Term Steps to Recovery

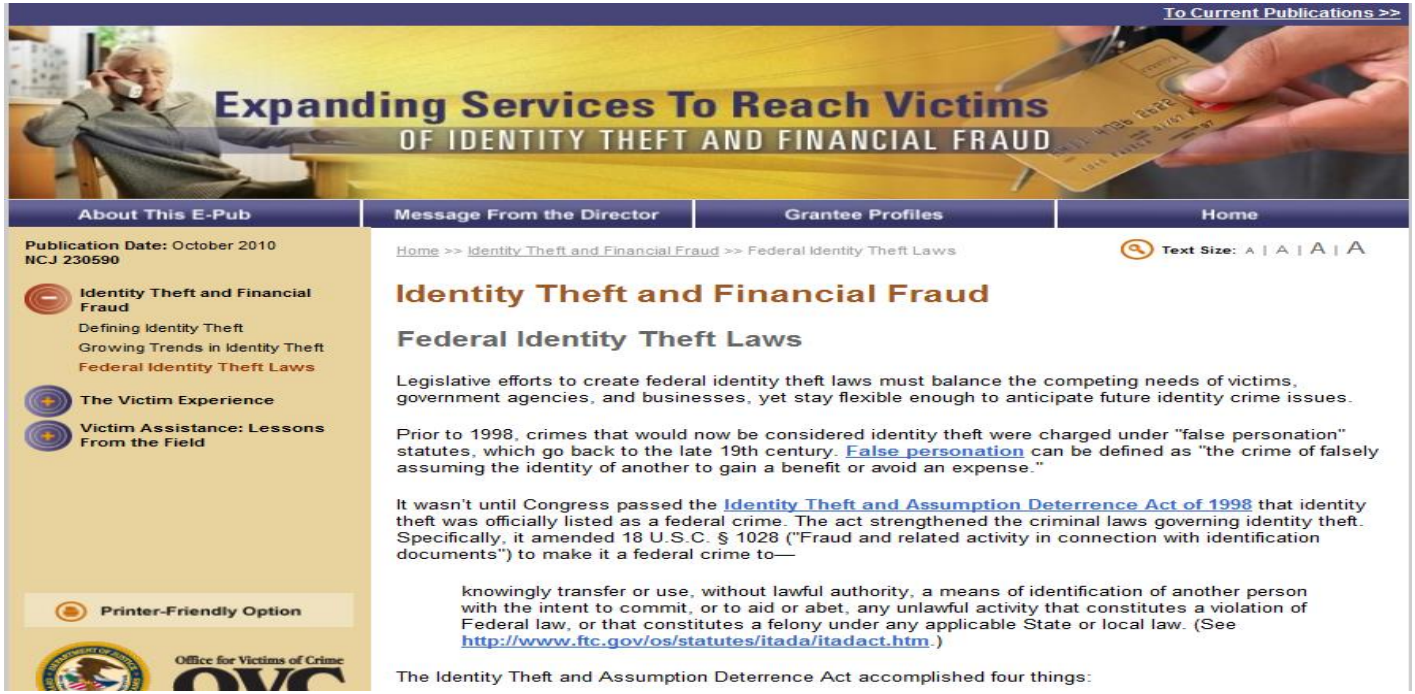
1. Consider an Extended Fraud Alert
2. Obtain Copies of Credit Report
   - Monitor Credit Reports
   - Disputing Fraudulent accounts and transactions by correcting reports
3. Credit Cards
4. Debt Collectors

# Extended Fraud Alert

- Lasts for 7 yrs
- 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*

# Online Training Course

- *Identity Theft Victim Assistance Online Training – Supporting Victims' Financial and Emotional Recovery*



To Current Publications >>

Expanding Services To Reach Victims
OF IDENTITY THEFT AND FINANCIAL FRAUD

About This E-Pub | Message From the Director | Grantee Profiles | Home

**Publication Date:** October 2010
**NCJ 230590**

- Identity Theft and Financial Fraud
  - Defining Identity Theft
  - Growing Trends in Identity Theft
  - Federal Identity Theft Laws
- The Victim Experience
- Victim Assistance: Lessons From the Field

Printer-Friendly Option

Office for Victims of Crime

Home >> Identity Theft and Financial Fraud >> Federal Identity Theft Laws

Text Size: A | A | A | A

## Identity Theft and Financial Fraud

### Federal Identity Theft Laws

Legislative efforts to create federal identity theft laws must balance the competing needs of victims, government agencies, and businesses, yet stay flexible enough to anticipate future identity crime issues.

Prior to 1998, crimes that would now be considered identity theft were charged under "false personation" statutes, which go back to the late 19th century. False personation can be defined as "the crime of falsely assuming the identity of another to gain a benefit or avoid an expense."

It wasn't until Congress passed the Identity Theft and Assumption Deterrence Act of 1998 that identity theft was officially listed as a federal crime. The act strengthened the criminal laws governing identity theft. Specifically, it amended 18 U.S.C. § 1028 ("Fraud and related activity in connection with identification documents") to make it a federal crime to—

> knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. (See http://www.ftc.gov/os/statutes/itada/itadact.htm.)

The Identity Theft and Assumption Deterrence Act accomplished four things:

# Resources for

- Department of Justice, Office for Victims of Crime, searchable database of victim service providers, http://ovc.ncjrs.gov/findvictimservices/
- National Crime Victim Law Institute (NCVLI) www.ncvli.org
- National of Victims' Rights Attorneys (NAVRA) www.navra.org

# Other Ways You Can Help!

- Provide identity theft prevention tips and recovery steps on your website.
  - Great example here: http://www.citywidebanks.com/information-security/identity-theft-prevent.html
- Have ID theft information available at your branches
- Understand emotional impacts

# Finally…

- Always remember: ***criminals choose to commit crime.***

- **Nothing you did, or did not do, gives a criminal permission to commit this crime.**

# Questions?