

# PREVENTING AND RECOVERING FROM IDENTITY THEFT

PRESENTED BY: INGER GIUFFRIDA,  
FINANCIAL EDUCATOR AND ASSET BUILDING CONSULTANT

September 29, 2016

# Identity Theft and the need for education

- *“High bankruptcy rates, increased credit card debt, and identity theft make it imperative that all of us take an active role in providing financial and economic education during all stages of one's life.”*

-Ruben Hinojosa

# Poll 1

- q.1. When is a young person likely to find out his or her identity has been stolen?

When:

- a. Opening an account at a bank or credit union
- b. Trying to get an auto loan
- c. Applying for an apartment
- d. Applying for a job
- e. Applying for a credit card
- f. Getting medical care
- g. None of the above
- h. All of the above

# Webinar purpose

---

- To provide people that serve young people in Maine in or transitioned from care with information on preventing and recovering from identity theft and the fraud committed with stolen identity information.

# What is identity theft?

---

*"But he that filches from me my good name  
Robs me of that which not enriches him  
And makes me poor indeed."*

- Shakespeare, Othello, act iii. Sc. 3.

# Identity theft—definition

- Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Definition from the U.S. Department of Justice

# How big is the problem?

- 6% of the reported incidences of Identity Theft in 2014 were from young people under the age of 20
- 18% were from 20 – 29 year olds
- Prevalence among foster youth is truly unknown, but believed to be **higher than average**

# How big is the problem?

- *“Identity theft is a serious crime that affects millions of Americans each year.”*

-Ben Bernanke



# Poll 2

- In your opinion, what is the most likely cause of a higher than average rate of identity theft among young people in care?
  - a. Poverty
  - b. Many people have access to their personal information
  - c. Frequent moves
  - d. No safe place to keep personal papers
  - e. Other

# How stolen identities are used

---

- Phone or utilities fraud
- Bank/finance fraud
- Government documents fraud
- Medical services fraud
- Other

# Dealing with identity theft

---

- Protect
- Detect
- Correct

# Poll 3

- What is considered identifying information?
  - a. Bank account numbers
  - b. Date, city, and state of birth
  - c. Passwords
  - d. Personal identification numbers
  - e. Immigration documents
  - f. None of the above
  - g. All of the above

# Protect

- Identifying information is anything that is specifically unique to you, such as your:
  - Credit card numbers
  - Debt card numbers
  - Bank account numbers
  - Driver's license number
  - Date, city, and state of birth
  - Social security number
  - Passwords or PINs
  - Immigration documents
  - Birth certificates

# Protect

- Keep identifying information somewhere safe
  - ▣ Challenges for young people in care or without a relatively permanent place to live
  
- Keep mobile device secure
  - ▣ Update software immediately and regularly
  - ▣ Change passwords and PINs
  - ▣ Use biometrics

# Good, not so good

- Passwords and PINs
  - Steven1
  - st3V3n2#!
  - 1126
  - 1qazxsw2
  - Password
  - !P34c3n0w\*

# Protect

- Passwords and PINs
  - CAPITALS, lowercase, numbers (1 2 3), and symbols
  - At least 10 characters long
  - No words that can be searched in a dictionary or names or places that can be associated with you
  - Change regularly (holidays)
  
- Security freeze



# Laws to protect young people

- Parents, legal guardians or other representatives of minors can place a security freeze on the minor's credit report
- ▣ Arizona, Connecticut, Delaware, Florida, Georgia, Illinois, Indiana, Iowa, Louisiana, **Maine**, Maryland, Michigan, New York, North Carolina, Oregon, South Carolina, South Dakota, Tennessee, Texas, Utah, Virginia and Wisconsin.

# Protect

- Sign up for account alerts
- Take data breach notifications **SERIOUSLY**
  - **1/5 data breach victims experienced fraud in 2015**
  - **Biggest problem: government agencies and healthcare organizations—a 64% increase in the rate of SSN exposure**
- Check credit reports regularly

# Laws to protect young people

- Child and Family Services Improvement and Innovation Act of 2011
- Mandating that all children in foster care, starting at age 14, receive a free consumer report each year until they leave the foster care system
- Child welfare must provide any assistance they need to interpret and resolve any inaccuracies in the report

# Protect

---

- Get help the minute fraud is detected
- Be alert for international transactions
- Secure or shred
- Look over your shoulder

# Protect

- Keep virus protection, spy- and malware protection, updated; update OS
- Be aware of your mail
- Never give out SS#
- Be aware online, at POS terminals, and in email

# Detect

- You don't get your bills or other mail.
- Merchants refuse your checks.
- Debt collectors call you or send you notices about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.
- Medical providers bill you for services you didn't use.

# Detect

- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- You are unable to enroll in any public benefits programs including MaineCare.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.

# Detect

- You get notice that your information was compromised by a data breach at a company where you do business or have an account.
- You are denied a job, a promotion, security clearance, a service, or an apartment.
- Withdrawals from your bank account that you can't explain.



# Liability limits for ATM and debit cards

- **Electronic Funds Transfer Act**
- If you report the loss of your card or number before it's used, your liability is \$0
- If you report the loss within 2 business days after you learn about the loss or theft, your liability may be up to \$50.
- If you report the loss between 2 and 60 business days after your statement is sent to you, your liability may be up to \$500.
- More than 60 days from when your statement is sent to you, your liability is unlimited.

# Liability limits for ATM and debit cards

- **Electronic Funds Transfer Act**
- If someone makes unauthorized transactions using your number, but your card is not lost, you are **NOT** liable for those transactions if you report them within 60 days.
- If you give someone your card or PIN, you are completely liable.

# Detect

- ❑ You get notice that your information was compromised by a data breach at a company where you do business or have an account.
- ❑ You are denied a job, a promotion, security clearance, a service, or an apartment.
- ❑ Withdrawals from your bank account that you can't explain.
- ❑ Unfamiliar charges on your credit card statement.

# Liability limits for credit cards

- **Fair Credit Billing Act**
- Maximum liability is \$50
- If loss of credit card or number reported before any use, liability is \$0
- If number is stolen but not the card, liability is \$0

# Discussion

---

- What are your thoughts about ATM, debit, and credit cards given this information?

# Detect—Under 18

- Adult care giver receives calls from:
  - ▣ collection agencies,
  - ▣ bills from credit card companies or medical providers, or
  - ▣ offers for credit cards or bank account checks in a child's name, even if the child has never applied for or used these services.
- Child or other family member is denied government benefits—another account using that Social Security number is already receiving benefits.

# Detect—Under 18

- The Social Security Administration, Internal Revenue Service, or some other government agency asks to confirm that a child is employed.
- The IRS notifies an parent/foster parent that the same information he or she filed for a dependent child is listed on another tax return.
- A child receives a notice from the IRS saying he or she failed to pay taxes on income the child has never received.

# Correct

1. Contact creditors of fraudulent accounts
  - ▣ Fraud department
  - ▣ Close or freeze account
  - ▣ Change logins, passwords, and PINs
2. Place fraud alert or credit freeze on credit records
  - ▣ Differences
3. File identity theft report with police
  - ▣ Get a copy
  - ▣ Issues
4. File an identity theft complaint for with the FTC
  - ▣ Keep a copy





FEDERAL TRADE COMMISSION

IdentityTheft.gov

[Log In](#)

 CHAT WITH OUR SUPPORT TEAM  
(mon-fri, 9am - 8pm EST)

What did the identity thief use your information for?

Select all that apply

Credit card accounts

Telephone, mobile, or utility accounts

Debit, checking, or savings accounts

Employment or taxes

Government benefits or IDs

Loans or leases

Other account types (Internet, insurance, securities, medical, etc.)



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Log In



CHAT WITH OUR SUPPORT TEAM  
(mon-fri, 9am - 8pm EST)

What did the  
identity thief get?

Select all that apply

government benefits

a driver's license

a passport

other government documents

← Previous

Continue →



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Log In



CHAT WITH OUR SUPPORT TEAM  
(mon-fri, 9am - 8pm EST)

1 Theft Details

2 Your Information

3 Suspect Information

4 Additional Information

5 Comments

6 Review Your Complaint

## Report Identity Theft to the FTC

Next, we are going to ask for specific details. We will use the information you provide to create your:

Identity Theft Affidavit



&

Recovery Plan



These will help you **fix problems** caused by identity theft.

Continue →

### How we handle your information

It's up to you to determine how much personal information you want to provide. The FTC enters this information into a secure online database that law enforcement agencies use in their investigations.

Please read our [Privacy Policy](#) to learn more about how we safeguard your personal information.

OMB Control Number: 3084-0047

← Start Over



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Log In



CHAT WITH OUR SUPPORT TEAM  
(mon-fri, 9am - 8pm EST)

1 Theft Details

2 Your Information

3 Suspect Information

4 Additional Information

5 Comments

6 Review Your Complaint

Fill in what you know. If you don't know, leave it blank.

## Fraudulent Driver's License

Which state issued the fraudulent driver's license?

When did you first notice the problem?

Month

Year

Select



Select



If you know, tell us when the fraudulent driver's license was created.

Month

Year

Select



Select



# Correct

- Close the new account
- Remove fraudulent charges
  - ▣ Call the fraud department of each business.
  - ▣ Explain that someone stole your identity.
  - ▣ Tell them which charges are fraudulent. Ask the business to remove them.
  - ▣ Ask the business to send you a letter confirming they removed the fraudulent charges.
  - ▣ Keep this letter. Use it if this account appears on your credit

# Correct

- Remove fraudulent charges from credit reports
  - ▣ Follow dispute procedures, but start with fraud departments
    - [Experian.com/fraudalert](https://www.experian.com/fraudalert)  
[1-888-397-3742](tel:18883973742)
    - [TransUnion.com/fraud](https://www.transunion.com/fraud)  
[1-800-680-7289](tel:18006807289)
    - [Equifax.com/CreditReportAssistance](https://www.equifax.com/CreditReportAssistance)  
[1-888-766-0008](tel:18887660008)

# Correct

- Contact the Social Security Administration to report misuse of SSN
  - Important if identification documents or any documents with SSN are involved in the theft
- Replace identification
- Change passwords and PINs
  - CAPITALS, lowercase, numbers (1 23), and symbols
  - At least 10 characters long
  - No words that can be searched in a dictionary or names or places that can be associated with you
  - Change regularly (holidays)

# Identity Theft Risk Assessment

- I receive several offers of pre-approved credit every week. **(5 points)**
- I do not shred the pre-approved credit offers I receive (cross-cut shredder preferred) before putting them in the trash. **(5 points)**
- I throw away old credit and debit cards without shredding or cutting them up. **(5 points)**
- I use an ATM machine and do not examine it for signs of tampering. **(5 points)**
- I do not have a P.O. Box or a locked, secured mailbox. **(5 points)**
- I carry my Social Security card in my wallet. **(10 points)**
- I use a computer and do not have up-to-date anti-virus, anti-spyware, and firewall protection. **(10 points)**
- I do not believe someone would break into my house to steal my personal information. **(10 points)**
- I use an unlocked, open box at work or at my home to drop off my outgoing mail. **(10 points)**
- I carry my military ID in my wallet at all times. (It may display my SSN.) **(10 points)**
- I do not shred my banking and credit information or tax information using a cross-cut “confetti” shredder, when I throw it in the trash. **(10 points)**
- I provide my Social Security number (SSN) whenever asked, without asking why it is needed and how it will be safeguarded. **(10 points)**
- **Add 5 points** if you provide it orally without checking to see who might be listening nearby.



# Identity Theft Risk Assessment

- I respond to unsolicited email messages that appear to be from my bank or credit card company. **(10 points)**
- I leave my purse or wallet in my car. **(10 points)**
- I have my driver's license number and/or SSN printed on my personal checks. **(10 points)**
- I carry my Medicaid or Medicare card in my wallet at all times. (It displays my SSN.) **(10 points)**
- I do not believe that people would root around in my trash looking for credit or financial information or for documents containing my SSN. **(10 points)**
- I do not verify that all financial (credit card, debit card, checking) statements are accurate monthly. **(20 points)**
- I do not regularly change my PINs or passwords or use the same PINs and passwords for multiple accounts. **(20 points)**
- I use words or numbers that are easily associated with me or common words or key strokes as passwords or PINs. **(20 points)**
- I use public WIFI or public computers to buy things online, review my bank account statements, or conduct other financial transactions. **(20 points)**
- I am or have been in foster care. **(20 points)**
- I do not have control over or know the location of my birth certificate, SSN card, or other key documents. **(20 points)**
- I have not ordered a copy of my credit reports for at least 2 years. **(20 points)**

# Identity Theft Risk Assessment

- 100+ points
  - ▣ You are at high risk for identity theft
- 50 – 99 points
  - ▣ Your risk for identity theft is average
- 0 – 49 points
  - ▣ Your risk for identity theft is lower than average, but remain vigilant

# Poll 4

- What is the result of your identity theft risk assessment?
  - a. Less than 49
  - b. Greater 50, but less than 100
  - c. Over 100

# Poll 5

---

- How do you feel about those results?
  - a. Great
  - b. Concerned, but in control
  - c. Yikes

# As a result of this webinar . . .

- What is one thing you are going to do differently to protect your own identity?
- What is one thing you are going to make sure the young people you work with know? Or can do differently?

# Why this problem will continue to be with us

- *“Criminals look at identity theft and say only 1 in 700 criminals gets convicted of it. And they look at check forgery and they know that for every 1,400 forgers arrested, only about 123 get convicted and about 26 go to jail. So the rewards are great, but the risks are very slim. So that's one of the reasons that make it very popular.”*

-Frank Abagnale

# Contact Information

47

- Inger Giuffrida, Consultant
- Phone: 405-819-7039
- Email: [inger.giuffrida@gmail.com](mailto:inger.giuffrida@gmail.com)

# Sources

---

- The Federal Trade Commission
- Identity Theft Resource Center
- Pew Charitable Trusts
- Keys to Your Financial Future
- Your Money, Your Goals
- National Conference of State Legislatures
- Department of Justice