Identity Theft
PLANNING FOR THE FUTURE
MAY 24, 2017
Welcome
Introductory Remarks

John Krebs
Division of Privacy and Identity Protection, Federal Trade Commission
General Information

- Please be aware that, if you leave the Constitution Center building for any reason during the conference, you will have to go back through security screening again.
- Restrooms are located in the hallway just outside conference room.
General Information

• Please be advised that this event is being webcast. By participating in this event, you are agreeing that your image, and anything you say or submit, may be posted indefinitely at ftc.gov or on one of the Commission’s publicly available social media sites.

• If you notice any suspicious activity, please alert building security.
Emergency Procedures

• If an emergency occurs that requires you to leave the Conference Center but remain in the building, follow the instructions provided over the building PA system.

• If an emergency occurs that requires the evacuation of the building, an alarm will sound. Everyone should leave the building in an orderly manner through the main 7th Street exit. After leaving the building, turn left and proceed down 7th Street and across E Street to the FTC Emergency Assembly Area. Remain in the Assembly Area until instructed to return to the building.
Submitting Questions and Comments

• During the conference
  – Please use the provided notecards and hand them to FTC staff

• Following the conference
  – Go to the Public Comments section of the conference event page
My Contact Information

John Krebs
Federal Trade Commission
jkrebs@ftc.gov
Opening Remarks

Maureen K. Ohlhausen
Acting Chairman, Federal Trade Commission
Setting the Stage: Identity Theft Today
Presenters

Keith Anderson, Bureau of Economics, Federal Trade Commission
Sean McCleskey, Director of Organizational Education and Measurement, Center for Identity, The University of Texas at Austin
Alana Benson, Identity and Document Fraud Consultant
Keith Anderson
Bureau of Economics, Federal Trade Commission
Identity Theft: What Do the Statistics Tell Us?

Keith B. Anderson  
Bureau of Economics  
Federal Trade Commission
Introductory Items

• The views expressed here are just mine and do not represent the views of the Federal Trade Commission or any of the Commissioners.
• The data I will present here are based on the results of the Bureau of Justice Statistics 2014 ID theft supplement to the National Crime Victimization Survey.
## Identity Theft, 2014

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Victims</th>
<th>Percent of Adult Population</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Victims</td>
<td>17,576,200</td>
<td>7.0%</td>
</tr>
<tr>
<td>Existing Accounts Misused</td>
<td>16,392,600</td>
<td>6.6%</td>
</tr>
<tr>
<td>New Accounts or Other Misuses</td>
<td>1,760,100</td>
<td>0.7%</td>
</tr>
<tr>
<td>New Accounts Opened</td>
<td>1,077,100</td>
<td>0.4%</td>
</tr>
<tr>
<td>Information Used in Other Ways</td>
<td>713,000</td>
<td>0.3%</td>
</tr>
</tbody>
</table>
Financial Costs of ID Theft

The Total – Social – Cost of an Incident of ID Theft

• No financial cost was reported in 35% of ID thefts.
  • This suggests that 4.5% of consumers were victims of an ID theft involving a financial cost.

• Looking just at those instances in which there was a financial loss, the median cost per ID Theft was $300.

• However, the losses from ID Theft are heavily skewed, with a limited number of incidents involving a much greater financial loss.
  • In 20% of incidents that involved a financial cost, the total social cost per incident was at least $1,000.
  • 10% of incidents involved social costs of at least $2,000 – more than 6 times the median value.
  • Almost ¾ of the total cost reported was accounted for by those incidents that involved the top 10 percent of loss per victim.
Financial Costs of ID Theft
Cost of an Incident of ID Theft That Was Borne by the Victim

• Not all of the costs resulting from ID Theft are borne by the victim.
• Indeed, only 13.8% of victims reported that they had paid money out of their own pocket in resolving the issue.
• Of those who incurred an out-of-pocket loss, the median amount was only $100.
• Again, these figures are highly skewed.
  • In the 20% of cases that involved the highest victim costs, the had out-of-pocket expenses of $600 of more.
  • In the 10% of cases that involved the highest victim costs, the victim paid at least $1,500.
# Financial Costs of ID Theft

(Median of Non-Zero Values)

<table>
<thead>
<tr>
<th></th>
<th>Social Cost</th>
<th>Cost to the Victim</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ID Theft</td>
<td>$300</td>
<td>$100</td>
</tr>
<tr>
<td>Misuse of Existing Credit Card</td>
<td>$300</td>
<td>$40</td>
</tr>
<tr>
<td>Misuse of a Checking or Savings Account</td>
<td>$200</td>
<td>$90</td>
</tr>
<tr>
<td>Misuse of an Other Existing Account</td>
<td>$200</td>
<td>$200</td>
</tr>
<tr>
<td>Opening New Accounts</td>
<td>$680</td>
<td>$300</td>
</tr>
<tr>
<td>Other Misuses</td>
<td>$1,000</td>
<td>$500</td>
</tr>
</tbody>
</table>
### Types of New Accounts and Other Misuses

<table>
<thead>
<tr>
<th>Type of New Accounts or Other Misuse</th>
<th>Number of Victims</th>
<th>Percent of New Account and Other Misuse Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Credit Card Accounts</td>
<td>531,800</td>
<td>30.2%</td>
</tr>
<tr>
<td>Fraudulent Tax Return Filed</td>
<td>261,300</td>
<td>14.8%</td>
</tr>
<tr>
<td>New Telephone Accounts</td>
<td>201,700</td>
<td>11.5%</td>
</tr>
<tr>
<td>New Loans or Mortgages</td>
<td>157,900</td>
<td>9.0%</td>
</tr>
<tr>
<td>False Information Provided to Police</td>
<td>120,500</td>
<td>6.8%</td>
</tr>
<tr>
<td>New Checking or Savings Account</td>
<td>104,000</td>
<td>5.9%</td>
</tr>
<tr>
<td>Used in Applying for a Job</td>
<td>77,300</td>
<td>4.4%</td>
</tr>
<tr>
<td>Used to Get Medical Treatment</td>
<td>74,900</td>
<td>4.3%</td>
</tr>
<tr>
<td>New Online Payment Accounts</td>
<td>66,7000</td>
<td>3.8%</td>
</tr>
</tbody>
</table>
### Types of New Accounts and Other Misuses (Continued)

<table>
<thead>
<tr>
<th>Type of New Accounts or Other Misuse</th>
<th>Number of Victims</th>
<th>Percent of New Account and Other Misuse Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Used to Rent an Apartment or a House</td>
<td>57,700</td>
<td>3.3%</td>
</tr>
<tr>
<td>Used to Apply for Government Benefits</td>
<td>53,000</td>
<td>3.0%</td>
</tr>
<tr>
<td>New Auto Insurance Policies</td>
<td>13,200</td>
<td>0.7%</td>
</tr>
<tr>
<td>New Medical Insurance Policies</td>
<td>12,000</td>
<td>0.7%</td>
</tr>
</tbody>
</table>
### Other Financial Problems Experienced by Victims of New Account and Other Misuses ID Theft

<table>
<thead>
<tr>
<th>Type of Problem Experienced</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit-related Problems</td>
<td>13.1%</td>
</tr>
<tr>
<td>Banking Problems</td>
<td>6.7%</td>
</tr>
<tr>
<td>Problems with Debt Collectors</td>
<td>14.0%</td>
</tr>
<tr>
<td>Legal Problems</td>
<td>3.3%</td>
</tr>
<tr>
<td>Problems with Utility Services</td>
<td>1.6%</td>
</tr>
</tbody>
</table>
Non-Financial Costs Borne by Victims

- Victims must spend time resolving problems resulting from having their ID stolen
  - At the time they were interviewed, just over a quarter – 27% – of victims of new account or other misuse ID theft indicated that they were still dealing with problems
  - Of those who had resolved all problems, 22% said that they had spent a month or more resolving their problems.

- Many victims also incurred emotional distress as a result of their experience.
  - 55% of victims of new account or other misuse ID theft said that they had experienced either moderate or severe emotional distress as a result
  - This is comparable with the percentage of those who had experienced an assault who said that they had experienced such levels of distress – 51 percent for simple assault and 60 percent for aggravated assault.
Who is More Likely to Become a Victim

- The prevalence of New Account and Other Misuse ID theft is highest among those aged 25 to 64. Among those of this age, about 0.8% were victims. This compares to 0.5% among those who were 65 or over and those between 18 and 24.
- While 0.8% of whites reported being a victim of this type of ID theft, the rates were somewhat higher for blacks or African Americans – 1.0% – and Hispanics or Latinos – 0.8%.
- There are no significant differences based on sex or income level.
Sean McCleskey
Director of Organizational Education and Measurement, Center for Identity, The University of Texas at Austin
IDENTITY THEFT TODAY
Identity theft is the fraudulent acquisition and use of a person’s personally identifiable information (PII)

- Financial Fraud (via Devices, Credit Cards, Checks, Bank access)
- Tax Identity Theft
- Synthetic Identity Theft (False ID)
- Immigration (Passport & Visa Fraud)
- Medical Identity Theft
- Cyber Intrusions
- Ghosting
Impact of Identity Theft is Big, Real and Diverse.

- Financial Loss
- Health Risks
- Increase in Other Crimes
- National Security Risks
- Reputation Damage
- Personal Security Risks

© 2017 Proprietary, The University of Texas at Austin, All Rights Reserved.
Proliferation of Identity Theft:
It is simple economics.
Profit potential is high and hidden

– Much higher than those for robbery, burglary, and street level drug dealing
– Businesses are willing to absorb “acceptable levels” of fraud loss
– Proceeds are easy to launder and conceal
Consequences are low

– These crimes are typically …
  • detected well after they are committed
  • often unreported
  • due to jurisdictional issues and scarce resources, often never investigated

– Declinations are frequent, sentences tend to be light
Identity crimes fund criminal enterprises

• These crimes are increasingly becoming the purview of organized criminal enterprises, many of which are transnational

• Often perpetrated by individuals and groups engaging in other more serious offenses to include narcotics trafficking, extortion, and murder for hire
Identity crimes facilitate other crimes

- Narcotics/Drug Trafficking
- Organized Crime
- Mail Fraud/Mail Theft (can be a precursor to ID crime)
- Mortgage Fraud
- Weapons trafficking
- Homicide
- Terrorism/National Security
- Wire Fraud
- Human trafficking
- Online Impersonation
- Revenge porn
- Extortion/blackmail
HOW IS IDENTITY STOLEN?


**UT CID Identity Threat Assessment and Prediction (ITAP)**

*ITAP* is a national analytical knowledge repository of identity theft and fraud cases occurring in multiple market sectors, including but not limited to DHS 16 critical infrastructure sectors.

ITAP is a computational model of “how Identity Theft and Fraud is done” identifying risks, vulnerabilities, consequences, solutions, and gaps to understand current threats and to predict future risks.
Where are the vulnerable points of entry?

Digital vs Non-Digital Theft

- Digital [46%]
- Non-Digital [53%]
- Both [1%]

Source: UT CID Identity Threat Assessment and Prediction (ITAP) project.
How is PII frequently stolen?

UT CID ITAP cases show common strategies...

- Physical theft - stolen wallets, purses, mail
- Phone and mail scams
- Dumpster diving and shoulder surfing
- Credit card skimming
- Email phishing
- Social engineering
- Using unprotected Wi-Fi networks
- Computer (Network/Software) breaches
Identity Theft “Steal Me” Flags
UT CID ITAP models WHO and WHEN Identity Theft and Fraud occurs.

- Insider Theft: 10.2%
- Hacking: 29%
- Third Party Vendors: 15.1%
- Employee Negligence: 10.9%
- Physical Theft: 12.5%
- Accidental Exposure: 11.5%
- Data on the Move: 7.9%
THE BIG PICTURE: We all are impacted … consumers, corporations, and governments around the world

• We must understand that recovery from the theft of an Identity asset is not just about replacing a new credit card or driver license.

• It can the sometime represent and insurmountable task of having to repair a lifetime of achievements.

• We need to capture more of these stories!
Do we really even understand what Identity is?

- Again we normally think of Identity Theft in terms of a financial crime, but are there other crimes?
- Is Identity replaceable?
- Is Identity an asset and what is it value?
UT CID Identity Ecosystem defines the “Physics of Identity”: its Contents (PII nodes), Connectedness, Identity Value, Liability, Rate of Change and so on.
Is Identity Replaceable?

• The theft of identity often is tied to a document, credential, or token.
• What about the path that leads to acquiring that item?
• Can you replace your reputation, good decisions, or your general standing in the world?
“To Protect a Thing is to Know a Thing”

• What is an identity asset?
• What is the value of an Identity asset?
• Who is looking to steal these identity assets?
• How are these identity assets compromised?
UT CID Identity Ecosystem Investigates Vulnerable “Entry” Points Given Breached PII.
“I AM NOT SURE WHAT I HAVE?!”

• What type of Identity assets do you hold?
• Where are those Identity assets located?
• Who has access to those identity assets?
• Are those identity assets monitored (analogue vs. cyber?)
MISCONCEPTIONS: Cyber Security is the Total Solution!

- The term cybersecurity is generically used to describe any issues related to the protection or unauthorized disclosure/theft of identity information.

  HOWEVER

- 50% of unauthorized disclosures/theft are not related to a machine or network

  -- according to UT CID ITAP research.
MISCONCEPTIONS:
Cyber Security is the Total Solution!

✓ There must be a TWO-FRONT fight! …
   People & Technology

✓ Not every identity thief is a hacker operating from a foreign country or government

✓ Network/Software security is incredibly important!

✓ But don’t forget People, Processes, and Policies.
WHAT CAN WE DO?

Research
Training
Awareness
Special Programs
More unbiased academic research is required to uncover the Identity Fundamentals.
Educate an Identity Workforce with the knowledge and skills to protect Identity ASSETS.
Who is the “Identity” Workforce?

- Everyone who uses PII to make decisions.
- Everyone who collects PII.
- Everyone who sells or trades in PII.
- Everyone charged with protecting PII and privacy.
- EVERYONE WHO TOUCHES PII.
- Everyone who looks and prosecutes the identity thieves and fraudsters.
Law Enforcement needs training to look for the right things in the right places

• What does a patrol officer typically look for?

• What should a patrol officer or investigator look for when hunting identity thieves and fraudsters?
  • Computers
  • Printers/ Scanners
  • Thumb/ Jump drives
  • Cell Phones
  • Card readers/ Encoders
  • Embossers
  • Laminators
What to look for ....
Is this evidence?
This is not an easy crime to investigate.

- Evidence of an identity crime may look innocuous and unimportant
- Unfamiliarity on the process to collect the evidence
- Limited knowledge of the laws available
- Don’t throw in the trash!!!
Combating Identity Theft

Creation of Financial Crimes/Identity Theft Task Forces: Comprised in most cases of Federal, State and Local agencies
South Texas Region

• Task Force created by USSS San Antonio Field Office to combat identity theft and major financial crimes

• Comprised of the following agencies:

Reduction in Identity-related Crimes

• The United States Attorney’s Office temporarily suspended loss requirement for case acceptance
• Intelligence was gathered on suspects with high rate of recidivism
• Education of prosecutors and the judiciary
• Outreach to business/organizations
Reduction in Identity-related Crimes

• Task Force being switched hours of operation and utilized drug warrants to initiate contact with suspects
• Worked closely with SAPD and Bexar County narcotics and gang units
• Cultivated contacts in the hotel/motel community
• FINALLY-use of the 1028A statute!!!
Prosecuting the Identity Thief and Fraudster
Identity Theft Penalty Enhancement Act

18 USC 1028A – Aggravated Identity Theft

. . . knowingly transfers, possesses or uses without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, . . .

. . . During and in relation to ANY felony violation
Identity Theft Penalty Enhancement Act

... Be sentenced to a term of imprisonment of 2 years.
Identity Theft Penalty Enhancement Act

... A court shall not place on probation any person convicted of a violation of this section ...
Identity Theft Penalty Enhancement Act

... No term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment ...
Case Study: Theft of data from a hotel

• Group of Aryan Brotherhood members and methamphetamine users stole credit card portfolios from storage facility in five-star hotel located in San Antonio, TX
• Hotel unaware of the theft
• 17,000 plus portfolios-contained CC #’s, CVC #”s, name, address of customers
• Information was utilized in conjunction with public sources to create counterfeit credit cards and fraudulent ID documents
Case Study:
Theft of data from a hotel

• Hotel unable to notify victims and comply with TX Business & Commerce Code
• Stolen information utilized to fund organized criminal organization
• Complete failure of hotel’s policies and procedures on securing identity information
• 1 Defendant (12 total) after release from prison was recently arrested 8 years later with thousands of the stolen portfolios still secreted for potential use
ID360 Scorecards from the Center for Identity helps organizations benchmark and improve.

- Unbiased
- Confidential
- Transparent
- Top-tier University
- Expert researchers and practitioners
Success in the future will rely on Research and Education.

- Understanding your identity vulnerabilities and risks
- Understanding the Identity Ecosystem
  - PII content, connectedness, value, liability, …
- Defining and measuring against best practice benchmarks
- Building a knowledgeable and skilled workforce
- Equipping law enforcement and prosecutors with knowledge and resources
R. Sean McCleskey, JD
Special Agent (Retired), U.S. Secret Service
Director of Organizational Education and Measurement

Center for Identity
The University of Texas at Austin
201 East 24th Street, POB 5.102
Austin, TX 78712
512.471.6152
210.875.4844

sean@identity.utexas.edu
Alana Benson
Identity and Document Fraud Consultant
State of New Hampshire
DEPARTMENT OF HEALTH AND HUMAN SERVICES
CERTIFICATE OF LIVE BIRTH

1. CHILD’S NAME (First, Middle, Last) ALANA RAE BENSON
2. DATE OF BIRTH [REDACTED]
3. TIME OF BIRTH 11:10 AM
4. SEX FEMALE
5. CITY, TOWN OR LOCATION OF BIRTH MANCHESTER
6. COUNTY OF BIRTH HILLSBOROUGH
7. PLACE OF BIRTH ELLIOT HOSPITAL
8. FACILITY NAME ELLIOT HOSPITAL
9. I CERTIFY THAT THIS CHILD WAS BORN ALIVE AT THE PLACE AND TIME AND THE DATE STATED
10. DATE SIGNED (Month, Day, Year) 5/24/19
11. SIGNATURE Stephen Null
12. CERTIFIER’S NAME AND TITLE GRIFFITHS, LINDA
13. ATTENDANT’S MAILING ADDRESS 500 TARTTOWN ROAD SUITE 105, MANCHESTER, NH 03103
14a. CITY/TOWN CLERK [REDACTED]
14b. CLERK’S NAME [REDACTED]
15. DATE FILED [REDACTED]
16. MOTHER’S NAME PENNY JO BENSON
17. DATE OF BIRTH [REDACTED]
18. BIRTHPLACE PENNSYLVANIA
19a. RESIDENCE-CITY, TOWN, OR LOCATION DERRY
19b. MOTHER’S SURNAME NOVACK
19c. COUNTY ROCKINGHAM
19d. STATE NEW HAMPSHIRE
20. MOTHER’S MAILING ADDRESS 03038
21. FATHER’S NAME LAWRENCE KENNETH BENSON
22. DATE OF BIRTH [REDACTED]
23. BIRTHPLACE NEW YORK
24a. I CERTIFY THAT THE PERSONAL INFORMATION PROVIDED ON THIS CERTIFICATE IS CORRECT TO THE BEST OF MY KNOWLEDGE AND BELIEF.
24b. SIGNATURE OF PARENT OR OTHER INFORMANT [REDACTED]
24c. RELATION TO CHILD MOTHER

ANY ERRORS, OMISSIONS, OR AMENDMENTS MADE TO THIS DOCUMENT WILL AUTOMATICALLY MAKE THIS FORM (CERTIFICATE) NULL AND VOID.
CERTIFICATE OF VITAL RECORD

The Commonwealth of Massachusetts
DEPARTMENT OF PUBLIC HEALTH
REGISTRY OF VITAL RECORDS AND STATISTICS

COPY OF RECORD OF BIRTH

REGISTERED NUMBER:
STATE FILE NUMBER:

CHILD

NAME: ALYSON
SEX: FEMALE
DATE OF BIRTH: 1991
PLACE OF BIRTH: MA

PLURALITY: SINGLE
TIME: 12:57 AM

MOTHER/PARENT

NAME: SARAH
SURNAME AT BIRTH OR ADOPTION: 
BIRTHPLACE: NY
AGE OR DATE OF BIRTH: 

FATHER/PARENT

NAME: ALBERT
SURNAME AT BIRTH OR ADOPTION: 
BIRTHPLACE: MA
AGE OR DATE OF BIRTH: 

AT-BIRTH RESIDENCE:
Identity at the Core
1. “Identities” are how agencies and institutions know us.

2. Agencies and institutions know our identities through documents.

3. Documents breed other documents: birth certificate > driver’s license > passport.
Apply for a Wyoming Driver’s License

To apply for a driver’s license in Wyoming, you must visit your local WY DOT office in person. You will need:

- Proof of your **identity**, such as your:
  - U.S. birth certificate.
  - U.S. passport (valid).
  - Citizenship certificate.

- Proof of your WY **residency** (2 documents), such as your:
  - Utility bill.
  - Bank statement.
  - Phone bill.

- Proof of your **Social Security number** (SSN), such as your:
  - Social Security card.
  - Bank statement.
  - W-2 form.
REAL ID COMPLIANT IDENTIFICATION AND RESIDENCY REQUIREMENTS
United States Citizens

To obtain a REAL ID COMPLIANT ORIGINAL NH Driver License or Non-Driver Identification Card, you must provide proof of identity, Social Security number and NH residency (legal physical address). You must provide these items even if you are transferring a compliant card from another state. Please see the bottom of the page for additional requirements needed for driver license applicants less than 18 years of age.

**IMPORTANT:** If your current name is different than your birth name on the document you are providing, you must also provide legal documentation (issued by a city, town, state, court or federal agency) to prove your name change, i.e., marriage certificate, civil union certificate or divorce decree.

1 OF THE FOLLOWING ITEMS TO SHOW PROOF OF IDENTITY and 1 OF THE FOLLOWING ITEMS TO SHOW PROOF OF SOCIAL SECURITY NUMBER and 2 OF THE FOLLOWING ITEMS TO SHOW PROOF OF NH RESIDENCY

- An original or certified copy of your birth certificate issued by a city, town, state, court or federal agency with a raised seal or stamp of the issuing authority (this would include US Citizens born abroad or a US Department of State issued birth certificate). **IF YOUR NAME HAS CHANGED FROM WHAT IS LISTED ON YOUR BIRTH CERTIFICATE, PLEASE SEE IMPORTANT INFORMATION ABOVE**
- Certificate of Naturalization
- A valid unexpired U.S. Passport or U.S. Passport Card

Please note: Driver Licenses or driver privilege cards from other States are not acceptable as proof of identification.

Documents indicated with a red arrow (➡️) must be dated within the last sixty (60) days

TRANSFERRING FROM ANOTHER STATE: The applicant’s out-of-state Driver License must be relinquished (RSA 263:4)

RENEWAL: Current Valid NH License ONLY or a NH license that has not been expired for more than one (1) year. If no photo/digital image is on file, the applicant will be treated as an original applicant

DUPLICATE: If photo/digital image is on file, nothing further is required. If no photo/digital image is on file, the applicant will be treated as an original applicant

UNDER 18: Driver Education Certificate, Parental Authorization Certificate, Driver’s Certification of Additional Supervised Driving are also required

Rev. 4/2017
Identity Verifying Documents
Identity Supporting Documents

W-2 Wage and Tax Statement

2014

Department of the Treasury – Internal Revenue Service

Employee's Social Security Number: 123-45-8789

Employee Identification Number: 11-2233445

The Big Company
123 Main Street
Anywhere, PA 12345

Jane A. DOE
123 Elm Street
Anywhere Else, PA 20456

Employee's Social Security No.: 123-45-8789

Employee's Ssn: 123-45-8789

Gross income:

W-2

Salary, wages, tips, etc.

1

12,500.00

Provided to Employee's FEDERAL Tax Return:

This information is being furnished to the Internal Revenue Service.

PA

12345

Due Date

11/2/2013

Amount Due

226.36

Service Address

12348 Main Street

Service From

9/7/2012

Service To

12/6/2012

Up to 2 things on all stamped checks

CUSTOMER ACCOUNT INFORMATION - RETAIN FOR YOUR RECORDS

WORLD'S PANAMA PACIFIC EXPOSITION IN SAN FRANCISCO

Mrs. Amber Haly Pipers
Reganee

Michigan
1. Find an appropriate obituary from an open state.
2. Order the death certificate first.
3. Use the death certificate to order the birth certificate.
Open vs. Closed

OPEN

WA

OH

KY

VT

CLOSED

ALL OTHER STATES
Open vs. Closed

*Vermont is pending vital record legislation to become a closed state

**New York is broken into New York state vital records and New York City’s five boroughs
How to Steal Identities with Documents

1. Find an appropriate obituary from an open state.
2. Order the death certificate first.
3. Use the death certificate to order the birth certificate.
<table>
<thead>
<tr>
<th>Birth</th>
<th></th>
<th>Death</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full name</td>
<td></td>
<td>Full name</td>
</tr>
<tr>
<td>Birth date</td>
<td></td>
<td>Death date</td>
</tr>
<tr>
<td>City and state of birth</td>
<td></td>
<td>City and state of death</td>
</tr>
<tr>
<td>Parents full names (including mother’s maiden name)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CERTIFICATE OF DEATH

STATE OF WASHINGTON
DEPARTMENT OF SOCIAL AND HEALTH SERVICES
VITAL RECORDS

CERITIFIED COPY OF DEATH CERTIFICATE

Date Issued: 1/20/2017

Name: Briana [redacted]
Gender: Female
Age: 14
Birthdate: 10/17/1990
City, Town or Location of Birth: Washington
Place of Birth: U.S.A.
Marital Status: Never Married
Surviving Spouse's Name: N/A
Surviving Children's Names: N/A
Surviving Parents' Names: N/A
Sex of Survivors: N/A
Surviving Spouse's Place of Residence: N/A
Surviving Children's Place of Residence: N/A
Surviving Parents' Place of Residence: N/A

Date and Place of Death: 10/17/1990
City, Town or Location of Death: Washington
Place of Death: U.S.A.
Cause of Death: [redacted]
Place of Burial: N/A
Date of Burial: 10/17/1990
Cemetery: N/A
Burial Place: N/A

Certified by: [redacted]
Date of Certification: 1/20/2017

Filed on: 10/17/1990
File Number: 5146

[Signature of Certifying Physician]

[Signature of Medical Examiner or Coroner]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]

[Signature of Vital Records]
CERTIFICATE OF LIVE BIRTH

Certificate Number: [Redacted] Date Issued: 02/02/2017

Given Names: BRIANNA
Last Name: [Redacted]

Date of Birth: [Redacted] 1990
Facility: [Redacted]
Place of Birth: [Redacted] WASHINGTON
Time of Birth: 09:46 P.M.
Sex: FEMALE

Mother's Maiden Name: [Redacted]
Place of Birth: WASHINGTON
Age: [Redacted]
Father's Name: *** NONE NAMED ***

County File Number: [Redacted]
Filing Date: 10/10/1990

Fee Number: 1764390841

DECEASED
# Kentucky Certificate of Death

**Applicant:**

- **Legal Name:** [Redacted]
- **Date of Birth:** 1989
- **County of Death:** [Redacted]
- **Occupation:** Cake Decorator
- **Street Address:** [Redacted]

**Decedent Information:**

- **Social Security Number:** [Redacted]
- **Place of Death:** [Redacted]
- **Marital Status:** Widowed
- **Race:** White
- **Hispanic Origin:** No, not Spanish/Hispanic/Latino

**Additional Information:**

- **Mother's Name:** [Redacted]
- **Father's Name:** [Redacted]
- **Date of Death:** 2017

---

**Note:**

- The face of this document has a colored background - not a white background.
- This document is a certified copy of a Kentucky certificate of death. It contains personal details such as the decedent's name, date of birth, occupation, and race. The social security number and other personal identifiers are redacted. The certificate also includes fields for the decedent's family members and additional identifying details.
<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child's Name</td>
<td>Heather</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>1989</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>Central Baptist Hospital</td>
</tr>
<tr>
<td>Mother's Maiden Name</td>
<td>Kentucky</td>
</tr>
<tr>
<td>Father's Name</td>
<td>Kentucky</td>
</tr>
<tr>
<td>Social Security Number</td>
<td>2740005</td>
</tr>
<tr>
<td>Age at time of Birth</td>
<td>26</td>
</tr>
<tr>
<td>Birthplace</td>
<td>Kentucky</td>
</tr>
<tr>
<td>Birthplace (State or Foreign Country)</td>
<td>Kentucky</td>
</tr>
<tr>
<td>Residence State</td>
<td>Kentucky</td>
</tr>
<tr>
<td>Residence County</td>
<td>234005</td>
</tr>
<tr>
<td>Residence City or Town</td>
<td></td>
</tr>
</tbody>
</table>

**Verification:**

I certify that the personal information provided on this certificate is correct to the best of my knowledge and belief.

Signature of Informant: [Signature]

Date: [Date]

Certifier's Name and Title: [Name and Title]
Identity Supporting Documents

W-2 Wage and Tax Statement

Residential Lease

Clause 1. Identification of Landlord and Tenant

Clause 2. Identification of Premises

Clause 3. Limits on Use and Occupancy

Clause 4. Term of the Tenancy

Clause 5. Payment of Rent
... is anyone actually doing this?

- The Paper Trip I-IV
- In a report to the VT legislature, cited examples from NJ, CA, OK, VT, CO, and many others.
- As with all fraud, we do not really know how much is happening.
… but isn’t someone checking?

- CSI Effect

- Even when verification occurs, the information agencies have access to is not complete.

Table 1: Types of Death Reports and Whether SSA Verifies Them

<table>
<thead>
<tr>
<th>Source of Death Report</th>
<th>SSA verification of death</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Beneficiary</td>
</tr>
<tr>
<td>State (EDRS)</td>
<td>No</td>
</tr>
<tr>
<td>Funeral directors</td>
<td>No</td>
</tr>
<tr>
<td>Family members</td>
<td>No</td>
</tr>
<tr>
<td>Post offices</td>
<td>Yes</td>
</tr>
<tr>
<td>Financial institutions</td>
<td>Yes</td>
</tr>
<tr>
<td>Centers for Medicare &amp; Medicaid Services</td>
<td>Yes</td>
</tr>
<tr>
<td>Department of Veterans Affairs</td>
<td>Yes</td>
</tr>
<tr>
<td>State (non-EDRS)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Source: GAO-13-574T
Thank you SSA!

- Social Security numbers were invented to keep track of Social Security beneficiaries. That number was then used by other agencies, specifically the IRS, to keep track of tax payer information.
<table>
<thead>
<tr>
<th>Numident</th>
<th>Full DMF</th>
<th>Partial DMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>❣ SSA’s record of Social Security beneficiaries, their SSNs, and relevant death data.</td>
<td>❣ Death information extracted from the Numident into a file for six federal benefit giving agencies.</td>
<td>❣ Social Security Act forbids sharing state reported data, so a new database is created excluding ~11 million deaths.</td>
</tr>
</tbody>
</table>
Why does the Partial DMF matter?

❖ Aside from the six agencies that pay federal benefits, the Partial DMF is what agencies and institutions use to confirm your identity.

❖ If agencies do verify identities, and the database they are using to do so is missing roughly 11 million identities, those agencies cannot be sure they are issuing benefits to real identities.

❖ Document fraud affects every agency and institution.
Using Benefits to Track Data

❖ Born in NJ
❖ Died in NH
❖ NH Vital Statistics reports death to Social Security Administration
❖ SSA stops payments and records death on Numident
❖ Death extracted from Numident, recorded on the Full DMF
❖ Because it was reported by NH, a state, it is NOT included on the Partial DMF
❖ NJ Dept. of Pensions continues to send checks because they do not have access to her death data.
Vermont’s H.111:

“The House of Representatives took a step toward overhauling the vital records system Wednesday with a preliminary vote to approve H.111, a bill that would require people to show identification to prove they are a relative or authorized representative of the person named on the record before they can receive a certified copy.”
Under current law, we are not authorized to share state death information with the DNP portal. Section 205(r) of the Social Security Act (Act) limits the purposes for which we may disclose state death information. While the Federal Improper Payments Coordination Act of 2015 (P.L. 114-109) requires us to share our death information with DNP, it did not amend section 205(r) of the Act to include authority for us to provide DNP State death information. Thus, we appreciate GAO's recommendation that "Congress should consider amending the Act to explicitly allow SSA to share its full death file with Treasury for use through the DNP working system." This recommendation also aligns with a proposal in the President's fiscal year (FY) 2017 Budget that would grant us the legal authority to share all our death information, including data from the states, with DNP.
Works Cited


Alana Benson | alanabenson10@gmail.com
Tracking the Use of Leaked Consumer Data

Presenters

Dan Salsburg
Christina Yeung
Office of Technology Research and Investigation, Federal Trade Commission
What Happens to Leaked Credentials?

Research question:
When consumer credentials are made public, does anyone use them?

Goal:
Design and conduct a study that tracks the attempted use of stolen consumer credentials
Study of Credential Use

1. Create ~100 consumer accounts
2. Post account data publicly
3. Track use of data
Fake Customer Data

1. Name
2. Address
3. Phone number
4. Email address
5. Password
6. Payment mechanism
   - Credit card number
   - Online payment account
   - Bitcoin wallet
# Posting of Fake Customer Data

<table>
<thead>
<tr>
<th>APRIL</th>
<th>MAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 18 19 20 21 22 23 24 25 26 27 28 29 30</td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18</td>
</tr>
</tbody>
</table>

- **Posting 1 on paste site**
- **Posting 2 on paste site**
- **End data Collection**
Posting One vs. Posting Two

- Same data, posted twice
- Different format and time of day

Posting 1: ~100 views

Posting 2: ~550 views
(Picked up by Twitter bot)
Monitoring of Data Usage

• Monitored for about three weeks
  – Week before Posting 1 (Pre-study control)
  – Week after Posting 1 (Week 1)
  – Week after Posting 2 (Week 2)

• Logged
  – Email account access attempts
  – Payment account access attempts
  – Credit card attempted charges
  – Texts and calls received by phone numbers
Time Before First Unauthorized Access Attempt

Posting 1

1.5 hours

Posting 2

9 minutes

#IDTheftFTC
Total Unauthorized Access Attempts

- Pre-Study: 1 attempt
- Week 1: 119 attempts
- Week 2: 1,108 attempts
Unauthorized Access Attempts by Account Type

- Email Services
- Credit Card Numbers
- Payment Accounts
Account Activity

Posting 1

Posting 2

0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Email Services

Credit Card Numbers

Payment Accounts


#IDTheftFTC
Email Account Access Attempts by Week

Number of Attempts

<table>
<thead>
<tr>
<th></th>
<th>Pre-Study</th>
<th>Week 1</th>
<th>Week 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Attempts</td>
<td>1</td>
<td>47</td>
<td>466</td>
</tr>
</tbody>
</table>
Email Access Attempts by Unique IP Addresses

(Likely underestimates access attempts)
Geolocation of IPs Used in Access Attempts

*IP addresses identified as suspicious by a freely available service

#IDTheftFTC
Credit Card Purchase Attempts

- Max: $2,697.75, at a clothing website
- Total amount within two weeks: $12,825.53
  - Includes multiple payment attempts
  - Includes preauthorization charges
- Noteworthy attempts:
  - Online dating service
  - Pizza place
  - Hotels
Amount Attempted per Charge

- $0 - $1: 137
- $1 - $5: 43
- $5 - $10: 32
- $10 - $20: 52
- $20 - $30: 19
- $30 - $50: 20
- $50 - $100: 17
- $100 - $1k: 1
- $1k - $2k: 1
- Over $2k: 1
Charge by Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Charges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retailers</td>
<td>164</td>
</tr>
<tr>
<td>Unknown</td>
<td>79</td>
</tr>
<tr>
<td>Gaming</td>
<td>59</td>
</tr>
<tr>
<td>Entertainment</td>
<td>39</td>
</tr>
<tr>
<td>E-payment service</td>
<td>36</td>
</tr>
<tr>
<td>Online tools</td>
<td>23</td>
</tr>
<tr>
<td>Food</td>
<td>12</td>
</tr>
<tr>
<td>Gift card</td>
<td>9</td>
</tr>
<tr>
<td>Charity</td>
<td>8</td>
</tr>
<tr>
<td>Travel</td>
<td>7</td>
</tr>
<tr>
<td>Mobile phone</td>
<td>3</td>
</tr>
<tr>
<td>Insurance</td>
<td>1</td>
</tr>
<tr>
<td>Investment</td>
<td>1</td>
</tr>
</tbody>
</table>
Additional Thoughts

• If you post it, they will use it
• Paste sites should be monitored by email and payment service providers
• Two factor authentication provides some protection against stolen credentials
• Merchants should consider refusing seriatim purchase attempts
Future work

• Analysis of email spam, text spam, and phone calls received by fake consumer email accounts

• Posting of consumer data in other ways that might attract different types of thieves

Have relevant research?

www.ftc.gov/OTech | research@ftc.gov
Contributors

• Sheryl Roth
• Phoebe Rouge
• Joe Calandrino
• Aaron Alva
• Justin Brookman
• Phillip Miyo

• Nicole Davis
• Aaron Kaufman
• Amber Howe
• Biaunca Morris
• Jonathan Aid
• Anne Blackman
BREAK
The Identity Theft Marketplace
Moderator

John Krebs, Division of Privacy and Identity Protection, Federal Trade Commission

Panelists

Danny Rogers, CEO, Terbium Labs

Robert Hoback, Assistant to the Special Agent in Charge, Criminal Investigative Division, United States Secret Service
Danny Rogers
CEO, Terbium Labs
Online Anonymity 101

How Tor Works: 2

- Alice
- Dave
- Bob

Step 2: Alice’s Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Hidden Services: 6

- Tor cloud
- Tor circuit
- IP: Introduction points
- PK: Public key
- cookie: One-time secret
- RP: Rendezvous point

Step 6: Bob and Alice proceed to use their Tor circuits like normal.
The “Dark Web”
The "Dark Web"

#IDTheftFTC
Is the “Dark Web” all bad?

--

Tor Funding

.onion Content

Legal 47.7%

Drugs 12.3%

Site Down 17.7%

Explicit 6.8%

Multiple Categories (Illicit) 6.5%

Pharmaceuticals 3.2%

Other Illicit Activity 1.5%

Hacking & Exploits 1.3%

Fraud 1.3%

Exploitation 1.0%

Downloadable 0.5%

Extremism 0.2%
What are they doing with this data?

- “Classic” Identity Theft (mortgages, loans, etc.)
- Tax Fraud
- Three-way ecommerce and other retail scams
Bloods gang used social media in money scheme, officials say

Updated May 3, 2017 8:18 PM
By: John Riley john.riley@newsday.com

Bloods gang members used social media images of stacks of cash and criminals lounging in hot tubs to lure hundreds of young people into a million-dollar counterfeit checking and debit card scheme, police and prosecutors said on Wednesday.
Impact: Subsidizing Geopolitical Interference

During the conspiracy, the FSB officers facilitated Belan’s other criminal activities, by providing him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by U.S. and other law enforcement agencies outside Russia, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers. Additionally, while working with his FSB conspirators to compromise Yahoo’s network and its users, Belan used his access to steal financial information such as gift card and credit card numbers from webmail accounts; to gain access to more than 30 million accounts whose contacts were then stolen to facilitate a spam campaign; and to earn commissions from fraudulently redirecting a subset of Yahoo’s search engine traffic.
Impact: Undermining Trust in the Internet
Robert Hoback
Assistant to the Special Agent in Charge, Criminal Investigative Division, United States Secret Service
ShadowCrew & Operation Firewall

- The concept of ShadowCrew (a “dark web” cybercrime chat forum) was developed in early 2002 during a series of chat sessions between cyber criminals. They came up with the idea of an eBay style business model and the subsequent vendor review system that introduced people in need of stolen data or counterfeit identification to verified sellers of such products.
- The ShadowCrew website also contained a number of sub-forums where the latest information about hacking tricks, social engineering, credit card fraud, virus development, scams, and phishing
- carderplanet.com owned by Dmitry Gubolov a.k.a. Script, a website primarily in the Russian language.
ShadowCrew & Operation Firewall

• Important to note that Shadowcrew was the forerunner of today's cybercrime forums and marketplaces. The structure, marketplace, review system, and other innovations that began with Shadowcrew laid the basis of today's underground forums and marketplaces.

• This was the beginning of the Secret Service beginning to focus on the dark web and underground marketplace for stolen financial information and PII/Identity Theft.

• Shadowcrew website was taken down in 2004 by the Secret Service – Criminal communities regrouped on Eurasian sites using the Shadowcrew concept.
Underground Forum Advertisement

- Advertisement on a dark web cyber crime forum for automated card vending shop 2pac.cc
2pac.cc Automated Card Vending Shop

- Automated websites for the sale of stolen credit cards
- Administered by cyber criminals
- Sell stolen cards obtained through skimming operations, online retail breaches and largescale point-of-sale breaches
- Customer support
- Refund Policy
Dark Web Recent Trends

• Cybercrime-as-a-Service (CaaS) or Malware-as-a-Service (MaaS) - i.e. Account Checkers
• Medical Records / Electronic Health Record Databases
• Institutions of Higher Learning / Educational Services
Recent Trends – Cybercrime-as-a-Service

- Sale of stolen credit cards
- Sale of compromised bank accounts
- Sale of malware
- Sale of “botnet” logs
- “Drop” services
- Exploit Kits
- DDOS services
- Bulletproof Hosting
- “Cashout” services
- Cybercrime tips
- Self-policing
Recent Trends – Cybercrime-as-a-Service

- It is lucrative, there is a market for it, and the risk is very low. The market is those criminals who are good at committing fraud but may not have had the ability in the past to create malware and write code.
- Exploit kits that steal credit card information, crack passwords or harvest credentials can be bought for the right price. Botnets can be rented if you are interested in constructing a DDoS attack, or you simply want to scam a business by threatening a DDoS attack unless they pay a ransom (scareware).
- By lowering the barrier to entry, anyone with rudimentary knowledge can suddenly use “top notch” malware to steal, hold files for ransom, or cause general havoc.
- THE DARK WEB MARKETPLACE = ONE STOP SHOPPING
Recent Trends – Medical Records/EHR Databases

• Health records have gone digital in the last seven years – If online theft continues to accelerate at the current pace, everyone in the U.S. will have had their health care data compromised
• Common theme - It is very lucrative. As a hospital administrator, how much do you think your patients medical records that contain PII (Personably Identifiable Information – Name, DOB, SS#) are worth on the criminal underground?
• Records contain not just your PII, but driver’s license #, credit card #’s and INSURANCE INFO (fraudulent billing and prescription fraud)
• Electronic Health Record Databases – Complete EHR databases can command $500,000 on the dark web.
• *Monetizing raw data such as PII is not new on the dark web, but EHR contains data that can be used to create new markets for fraudulent tax returns, fake ID’s, birth certificates, stolen prescriptions = Synthetic Fraud*
Recent Trends – Educational Services

- Research studies across myriad disciplines conducted at universities put them in the sights of state-affiliated groups.
- However, according to Verizon, breach findings showed that over half involved the compromise and disclosure of **stored personal information** of both students and employees, while only a little over a quarter resulted in the disclosure of intellectual property.
- Criminal actors want your PII info to sell on the dark web and what better place to obtain it than your school personnel files?
- Phishing via email was the most prevalent variety of social attacks, while use of **stolen credentials** against web applications was the dominant hacking tactic.
Account Checkers

- Account checkers are basic brute force tools that test emails and passwords against a company website in order to validate accounts.
- Most likely over 20 sites/domains on the dark web that offer account checkers for approximately 85 well-known businesses (retail, hospitality, home improvement – ecommerce and brick and mortar)
Popular Account Checking Toolkits (Private Keeper & Sentry MBA)
Popular Account Checking Toolkits (con’t)

- Increase of account checkers over the past year on dark web forums – why?
- Recent massive database leaks (Yahoo/LinkedIn) leads to increase in “combo lists” (compromised user names and passwords) for sale on dark web. Attackers can attempt to reuse against other sites
- The data base info/”combo lists” are widely circulated among underground actors who use it in conjunction with account-checker tools
SLILPP.BIZ Homepage
## SLILPP.BIZ Homepage

![SLILPP.BIZ Homepage](image)

### New shops accounts

<table>
<thead>
<tr>
<th>Shop</th>
<th>Balance</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>HL</td>
<td>$2.00</td>
<td>$1.30</td>
</tr>
<tr>
<td>FEDEX</td>
<td>$2.00</td>
<td>$1.30</td>
</tr>
<tr>
<td>MAILS</td>
<td>$0.20</td>
<td>$1.30</td>
</tr>
<tr>
<td>STAMPS</td>
<td>$2.00</td>
<td></td>
</tr>
<tr>
<td>T-MOBILE</td>
<td>$2.50</td>
<td></td>
</tr>
<tr>
<td>UNIBET</td>
<td>$1.00</td>
<td></td>
</tr>
<tr>
<td>UPS</td>
<td>$2.00</td>
<td></td>
</tr>
<tr>
<td>USPS</td>
<td>$2.00</td>
<td></td>
</tr>
</tbody>
</table>

### HUGE Update

We are glad to introduce you a **brand new Other Shops** section! Additional information, more detailed search criteria and, of course, much more profit from accounts with the necessary information.

Have a nice shopping!

Представляем Вам полностью обновлённый раздел **Other Shops**! Дополнительная информация, более подробные критерии поиска и, конечно же, гораздо больше пользы от аккаунтов с необходимой информацией.

Приятного покупки!

---

#### Prices

<table>
<thead>
<tr>
<th>Shop</th>
<th>Price</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATT</td>
<td>$4.50</td>
<td>Wireless</td>
</tr>
<tr>
<td>TIGERDIRECT</td>
<td>$0.40</td>
<td>all</td>
</tr>
<tr>
<td>NEWEGG</td>
<td>$0.40</td>
<td>all</td>
</tr>
<tr>
<td>FUNICUL</td>
<td>Free</td>
<td></td>
</tr>
</tbody>
</table>

---

Copyright © 2012-2015 SLILPP

---

#IDTheftFTC
Only the Finest Customer Support
The Identity Theft Marketplace Moderated Discussion
The Impact of Identity Theft: The Big Picture
Moderator

Mark Eichorn, Division of Privacy and Identity Protection, Federal Trade Commission

Panelists

Ann Patterson, Senior Vice President, Program Director, Medical Identity Fraud Alliance

Christopher Mascaro, Vice President, Threat Intelligence & Analytics, First Data Corporation

Michael Beebe, Director, Return Integrity & Compliance Services (RICS) and IRS Security Summit Executive Lead, Internal Revenue Service

Todd Egaas, IRS Executive Official, Identity Theft Tax Refund Fraud ISAC, Internal Revenue Service

Kenn Kern, Chief of Staff to the Investigative Division and Special Assistant for International Relations, New York County District Attorney’s Office

#IDTheftFTC
Kenn Kern
Chief of Staff to the Investigative Division and Special Assistant for International Relations, New York County District Attorney’s Office
STRUCTURE OF THE OFFICE

• Investigation Division
  – Cybercrime and Identity Theft Bureau
    • High Technology Analysis Unit
    • Cyber Intelligence Unit
  – Financial Fraud Bureau
  – Major Economic Crimes Bureau
    • Financial Intelligence Unit
    • International Money Movement Center
  – Rackets Bureau
  – Tax Crimes Unit
  – Asset Forfeiture Unit
  – Public Corruption Unit
  – Investigation Bureau
THE CYBERCRIME AND IDENTITY THEFT BUREAU

- Cybercrime or identity theft related charges make up over 25% of all felony complaints
- District Attorney Vance created the Cybercrime and Identity Theft Bureau in 2010
  - 15 full-time ADAs
  - 90 additional Trial Division ADAs
  - 15 analysts
- Provide training to other parts of the Office
- The Bureau also includes an in-house lab for computer, phone, and other digital forensic work
- Cyber Intelligence Unit conducts long-term, strategic investigations into high-value targets
How Thieves Commit Fraud

• Recent arrest on May 3, 2017

• 39 defendants

• Theft of over $1 million through counterfeit check cashing
How Thieves Commit Fraud

Debit Card Cracking Scheme:

- **CHECK CASHERS**: Stolen account information
- **“PLUGS” (Ringleaders)**: Counterfeit checks
- **RUNNERS**: Account deposits and withdrawals

**RECRUITERS**
Complexity of Identity Theft Cases

• The Defendants gained control of legitimate StubHub accounts, fraudulently purchased e-tickets for popular events, resold the tickets, and then laundered the money internationally.

• Victimized more than 1,600 StubHub users and credit card accountholders.

• Charged with Money Laundering, Grand Larceny, Criminal Possession of Stolen Property, and Identity Theft, among others.
Collaboration and Partnership

GLOBAL CYBER ALLIANCE

CITY OF LONDON POLICE

POLICE DEPARTMENT CITY OF NEW YORK

Royal Canadian Mounted Police

AGC SINGAPORE ATTORNEY-GENERAL’S CHAMBERS

#IDTheftFTC
Barriers to Investigation: Encryption
LUNCH
The Victim’s Perspective
Moderator

Lisa Schifferle, Division of Consumer and Business Education, Federal Trade Commission

Panelists

Amy Wang, Identity Theft Victim
Tamera Fine, Assistant United States Attorney, District of Maryland
Eva Velasquez, CEO, Identity Theft Resource Center
Ellen Abbott, Manager, Consumer Investigations, Identity Theft & Breach Notification, Kroll
Tamera Fine
Assistant United States Attorney, District of Maryland
Dangers to Victims – Financial Fraud

- Dangers flow from the way the identities are being used.
  - Huge variance in how much harm is sustained by financial fraud victims.
  - Generally these variances fall into established patterns, but...

  ....there are always outliers and we must always remain open to assisting victims who are the unlucky few percent of victims who sustain lasting harm.
Dangers to Victims – Financial Fraud

- Some types of financial fraud, such as account takeovers, auto and home purchases, are generally easily resolved, due to records maintained by the creditor.
- New Accounts require significantly more effort to resolve.
- Utilities and Services are notoriously difficult to convince that you have been a victim, as are rental management companies.
- There are groups, such as the Felony Lane Gang out of Florida, which specifically target bank accounts, which often result in victims losing access not to credit, but to their own funds.
Dangers to Victims – Financial Fraud

• Just as financial fraud targets banks and businesses, benefits fraud targets the deep pockets of Uncle Sam. Benefits fraud includes:
  – Stolen Identity Refund Fraud (SIRF)
  – Unemployment, Social Security Retirement and Disability.
• This fraud diverts funds from the victims to the perpetrator.
• Whether it is a tax refund you are expecting and don’t get, or a social security check that gets diverted into another account, these disruptions can cause significant hardship, even if the funds are eventually restored.
• In addition, benefits can be cancelled due to an identity thief earning income using the victim’s identity.
Dangers to Victims – Employment

- Anywhere there is a large illegal immigrant population, there is use of other’s identities for employment purposes. This use can create big issues for victims:
  - Tax Issues
  - Benefits issues
  - MVA/DMV suspensions and revocations
  - Criminal Warrants
Dangers to Victims – “Collateral” Impacts

- Even financial fraud and use of a stolen identity for employment can have massive collateral consequences for victims:
  - Inability to get a job.
  - Inability to pass a background check.
  - Loss of security clearance.
Dangers to Victims – Medical Identity Theft

- One of the most devastating forms of identity theft is medical identity theft
  - Medical treatment is obtained using stolen health insurance information, or sometimes “on credit.”
  - The residual unpaid bills are the least of the problem.
  - The victim’s medical record becomes “polluted” with information about the health conditions, medications, and treatments of the identity thief.
  - In emergency situations, this has potential catastrophic consequences.
Dangers to Victims – Medical Identity Theft

• Identity Theft of Medical Credentials
  – We have had examples of people who pose as medical professionals, including treating patients and prescribing medications.
  – Here, again, access to what seems like insignificant personal details can greatly assist in the identity theft: where the victim went to school, what states they are licensed in, where they have practiced in the past.

• In addition to the danger this form of identity theft poses to the reputation and license of the medical professional, think of the potential of harm to the public.
Dangers to Victims – Criminal Activity

• Many career criminals use stolen identities because they have warrants outstanding.
• If caught, they give the fraudulent identification information.
• Stolen identities are often used to commit new crimes, such as check fraud schemes.
• When the scheme unravels, law enforcement comes after the name on the fraudulent account – the victim.
Dangers to Victims – Criminal Activity

• The problem of erroneous arrest of identity theft victims has become so significant that states are taking steps to “authenticate” identity theft victims to law enforcement.
• Use of stolen identities to avoid SORNA reporting requirements is common.
• Identity theft victims have been placed on terrorist watch lists and even forcibly removed from airplanes.
Contact Information

- Assistant U.S. Attorney (AUSA)
  Tamera Fine
- 410-209-4806 (work)
- 410-961-4502 (cell)
- tamera.fine@usdoj.gov
Eva Velasquez
CEO, Identity Theft Resource Center
The Aftermath: In their own words

• “One of the worst ways identity theft has affected me is the ongoing feeling of persecution. Not being able to trust ANYONE and being borderline paranoid when anyone asks for ANY personal information for any reason even when it is business related.”

• “I am always in fear about what will happen next, and who my information will get sold to.”

• “The identity theft was a bewildering, stressful experience. Since I don’t know who perpetrated the theft, I worry that he/she could use my information to victimize me again.”
Emotional Reactions

- Frustration/Annoyance (81%)
- Fear for financial security (69%)
- Rage or Anger (58%)
- Powerlessness/helplessness (54%)
- Loss of ability to trust (51%)
- Isolation (31%)
- Shame or embarrassment (28%)
- Suicidal (8%)
Behavioral and Physical Reactions

- Sleep disturbances (42%)
- Inability to concentrate (39%)
- New physical illness (29%)
- Loss of appetite (21%)
- Start or relapse of unhealthy or addictive behaviors (15%)
- Unable to work (10%)
Lost Opportunity Costs

- Spent time away from other life experiences (39.9%)
- Took time off work (28.8%)
- Spent time away from family (26.3%)
- Delayed educational opportunities (16.7%)
From a household to our nation:

- The ripple effect that directly impacts you

  - Borrowed money from family/friends (35%)
  - Closed existing online accounts (23%)
  - Used online accounts less frequently or not at all (33%)
  - Applied for government benefits (17%)
The Aftermath: In their own words

• “The thief was my landlord; hence I had to go to the Sheriff’s office to get assistance in gaining access to what was left of my personal property. I spent hundreds of dollars in legal paperwork, a mover, hotel rooms I had to live in until procuring another place to rent.”

• “I have been forced to do my income tax separate from my spouse at a higher bracket.”

• “Used my name for medical treatment. I was assessed with unpaid taxes, medical bills, and my medical record corrupted. I have yet to be able to get her information off my medical records.”
The Victim’s Perspective

Moderated Discussion
Resources for Recovery
Moderator

Ryan Mehm, Division of Privacy and Identity Protection, Federal Trade Commission

Panelists

Nat Wood, Associate Director, Division of Consumer and Business Education, Federal Trade Commission
Laura Ivkovich, Policy Analyst, Office for Victims of Crime, U.S. Department of Justice
Eugenia Buggs, Vice President, Global Marketing, Identity and Digital Protection Services, Generali Global Assistance
Nat Wood
Associate Director, Division of Consumer and Business Education, Federal Trade Commission
Report identity theft and get a recovery plan

Get Started ➔

IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:

Tell us what happened.
We'll ask some questions about your situation. Tell us as much as you can.

Get a recovery plan.
We'll use that info to create a personal recovery plan.

Put your plan into action.
If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

Get started now. Or you can browse a complete list of possible recovery steps.

#IDTheftFTC
Which statement best describes your situation?

- I want to report identity theft.
- Someone else filed a tax return using my information.
- My information was exposed in a data breach.
- Someone got my personal information or my wallet, and I'm worried about identity theft.
- Something else.
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.)
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 Report & Recovery Plan

These will help you fix problems caused by identity theft.

Continue ➔
Identity Theft Report

I am the victim of identity theft. This is my official statement about the crime.

Contact Information

Jane May Smith
100 Main Street
Washington, DC 20405
202-876-5309
janemay.smith@email.com

Personal Statement

I received a credit card bill from Chase, even though I've never had a credit card with Chase. I called and the bank said I needed to fill out an identity theft report. Just a few days later, I got a call from Verizon about buying a new iPhone. I told them I didn't buy an iPhone. Someone else had gone to a store in New Jersey and added two new lines to my account.

Accounts Affected by the Crime

<table>
<thead>
<tr>
<th>Credit card opened by the thief</th>
<th>Mobile phone with fraudulent charges (account takeover)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Company or Organization:</strong> Chase</td>
<td><strong>Company or Organization:</strong> Verizon Wireless</td>
</tr>
<tr>
<td><strong>Account Number:</strong> 9888888888</td>
<td><strong>Account Number:</strong> 547000089</td>
</tr>
<tr>
<td><strong>Date fraud began:</strong> 1/15/16</td>
<td><strong>Date fraud began:</strong> 1/15/16</td>
</tr>
<tr>
<td><strong>Date I discovered it:</strong> 3/15/16</td>
<td><strong>Date I discovered it:</strong> 3/15/16</td>
</tr>
<tr>
<td><strong>Total fraudulent amount:</strong> $400</td>
<td><strong>Total fraudulent amount:</strong> $900</td>
</tr>
</tbody>
</table>
Your Report is not submitted yet.

Almost Done! We recommend creating a free account so you can:

- Get a personal recovery plan that tracks your progress
- Print prefilled letters & forms
- Return anytime to update and view your affidavit
- Save time if this ever happens again

Yes, submit and create account ➔

No thanks, submit without an account

I understand that I will NOT be able to make updates.

Instead, I will receive a one-time copy of my affidavit and recovery plan.
Great. Your account has been created!

Here's your personal recovery plan. We'll guide you through each step.

Your Recovery Plan

- Call Bank of America to report the fraudulent account.
- Place a fraud alert on your credit reports.
- Review your credit reports for fraud.
- Send a follow-up letter to Bank of America.
- Consider placing an extended fraud alert or credit freeze.

Hide Completed Items

Report identity theft to the FTC.

#IDTheftFTC
Send a follow-up letter to Bank of America.

Completed?  Tasks

☐  Send a letter to Bank of America disputing the fraudulent account.

We've created a letter for you based on the information you've already provided.

Review and Print letter

☐  When did you mail the dispute letter?

Year  Month  Day
Select  Select  Select
November 19, 2015
Pat Smith
123 Maple Street
Washington, District of Columbia 20001

ABC Lending Corp.
678 Elm Street
Washington, District of Columbia 20001

RE: Disputed Account – Notice to Furnisher
987654321

Dear Sir or Madam:

On November 19, 2015, I notified you that I am a victim of identity theft and requested that you do the following:

- Close the unauthorized account
- Remove any charges on the unauthorized account, and
- Take steps to remove information about this account from my credit files.

I still have not received written confirmation of these actions. As I stated before:

I am a victim of identity theft, and I am writing to dispute certain information you have reported about me to the credit reporting agencies (CRAs). I recently learned that my personal information was used to open an account at your company. I did not open nor authorize this account, and I request that it be closed immediately. Please send me written confirmation that I am not responsible for charges on this account, and take appropriate steps to remove information about this account from my credit files.

I have enclosed a copy of my FTC Identity Theft Affidavit and my credit report showing the fraudulent account. Because the information you are reporting is inaccurate and the result of identity theft, I request that you stop reporting this information to the CRAs, as directed by section 628(c)(3)(B) of the Fair Credit Reporting Act, 15 U.S.C. §1681t(a)(3)(B). I ask that you take these steps as soon as possible.

I also have enclosed a copy of the FTC’s Notice to Furnishers, which explains your responsibilities when reporting information to CRAs. Please stop reporting this fraudulent information, investigate the matter, and delete any disputed items as soon as possible.

Please send me a letter explaining your findings and actions.

Sincerely,
Pat Smith

Enclosures:
- Identity Theft Affidavit
- Proof of identity
- Copy of Credit Report indicating information to be corrected
- FTC Notice to Furnishers of Information
Correct your Equifax credit report.

Completed? Tasks

☑ Write to Equifax. We’ve created a letter for you based on the information you’ve already provided.

Review and Print letter

☑ When did you mail the dispute letter?

Year: 2016  Month: January  Day: 18

Thanks. When you hear back from Equifax, come back and let us know what happened. If we haven’t heard anything in 28 days, we’ll send you a reminder.

☐ Did Equifax correct your credit reports?

® Yes
® No

Save and Go Back to Your Plan
January 20, 2016

Jane Smith
123 Main Street
Washington, DC, USA 20000

Equifax Consumer Fraud Division
P.O. Box 740296
Atlanta, GA 30374

RE: Request to Block Unauthorized Charges from Credit Report under FCRA 605B

Dear Sir or Madam:

I am a victim of identity theft. The information listed below, which appears on my credit report, is the result of identity theft.

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Account Number</th>
<th>Charge</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citibank</td>
<td>12345678</td>
<td>$607.00</td>
<td>10/2015</td>
</tr>
</tbody>
</table>

I have enclosed my Identity Theft Report, proof of your identity and a copy of my credit report showing the fraudulent items. Please block this information from my credit report, as directed by section 605B of the Fair Credit Reporting Act, and notify all furnishers of this information.

I appreciate your prompt attention to this matter, and await your reply.

Sincerely,

Jane Smith

Enclosures:
- FTC Affidavit and police report (Identity Theft Report)
- Proof of identity
- Fair Credit Reporting Act Section 605B
Laura Ivkovich
Policy Analyst, Office for Victims of Crime, U.S. Department of Justice
Presentation Overview

- What is OVC?
- How can OVC Help?
- Victims of Crime Act Funding (VOCA)
- Victim Services Available (In person and On line)
- National ID Theft Victim Assistance Network (NITVAN)
- Benefits of Collaboration/Force Multipliers
Office for Victims of Crime (OVC)

• In 1982, President Reagan established the President's Task Force on Victims of Crime,
• Task Force charged with assessing the treatment of crime victims throughout the Nation,
  – "The innocent victims of crime have been overlooked, their pleas for justice have gone unheeded, and their wounds—personal, emotional, and financial—have gone unattended."
• Task Force recommendations resulted in:
  – Victims of Crime Act (VOCA) enacted in 1984
  – VOCA establishes the Crime Victims Fund 1985
  – 1988 amendment to VOCA formally establishes the Office for Victims of Crime
VOCA

• Victims of Crime Act of 1984:
  – VOCA authorizes OVC to use monies from the Crime Victims Fund to support a number of programs that assist crime victims, including:
    • State Victim Assistance programs (formula)
    • State Compensation programs (formula)
    • Discretionary programs
# VOCA Authorized Activities

### Crime Victim Compensation (formula)
- To states to fund direct payments for crime victims
- Reimbursement for crime-related expenses (e.g., medical, mental health counseling, funeral and burial, lost wages, and loss of support)

### Victim Assistance Services (formula)
- To states for community-based victim service programs
- Supports the delivery of direct services (e.g., counseling, legal advocacy, etc.)

### Discretionary Activities
- National scope training and technical assistance
- Demonstration programs
- Victims’ legal assistance
- Program evaluation
- Fellowships
- Services to victims of federal crimes (e.g. Tribal Victim Assistance)
VOCA Funding Appropriations Cap Raised
States See Quadruple Rise in Victim Assistance Grant Funding

• VOCA Cap:
  – FY 14 - cap was $745 Million
  – FY 15 - cap went up to $2.361 Billion
  – FY 16 - cap went up to $3.042 Billion *

• OVC Awarded:
  – FY 14 - $456 million in state victim assistance grants
  – FY 15 - $1.9 billion in state victim assistance grants
  – FY 16 - $2.2 billion in state victim assistance grants

  – * VOCA statute expands use of federal funds to include “victim services,” in addition to the current authority for demonstration projects, program evaluation, compliance efforts, and training and technical assistance services.
OVC Online Directory of Victim Services

Welcome to the Online Directory of Crime Victim Services, a resource from the Office for Victims of Crime (OVC). Since its launch in 2003, the Directory has helped thousands of crime victims and service providers find nonemergency crime victim service agencies in the United States and abroad.

You can search the Directory by—
- location
- type of victimization
- service needed
- agency type

Are you a victim service program or organization? More than 10,000 programs are listed in the Directory and yours could be too. Add your program to the Directory and increase your program profile with providers and crime victims. Find out how on the Get Posted page.

The information provided in the directory is the sole responsibility of the not-for-profit programs and public agencies that chose to make this information publicly available on the Web. OVC does not endorse any particular products or services listed in this directory. See the Disclaimer page for more information.
National ID Theft Victim Assistance Network (NITVAN)

- State Victim Resources (numbers, links)
- Laws including Civil Suits, Access Devices, Cyber Crimes, Security Breaches
- Security Freeze Law & State-Specific ‘How To’s’
- ID Theft Passport Law
- Inclusion in state’s restitution definitions

- ovcttac.gov/identitytheftnetwork
- Twitter.com/IDTheftNetwork
- Facebook.com/IdentityTheftNetwork
NITVAN Resources You Can Use Now

• Printable Outreach Material
  – Brochures
  – Website Material
  – PSA Scripts & Audio & Visual Samples
• Quick Tip Sheets
• Ready-To-Use Forms
• Sample MOU’s
• Training Slides, Instructor Manuals, Worksheets
• NITVAN II – New OVC Funding…
  – Adding 20 additional coalitions to the network (3-yr project) – competitive $50,000 sub-awards
  – Training and TA as well as policy assistance
  – Guidance to the new and existing programs and coalitions… with an emphasis on cybercrime identity theft victims
  – Force multiplier – help expand the outreach and capacity of victim service programs to better address the rights and needs of victims of identity theft through the establishment of collaborative regional, statewide, or community-based coalitions dedicated to improving the response to victims of id theft
OVC - Online Interactive Training for Advocates

www.ovcttac.gov/IdentityTheft
ID Theft Help Mobile App

Features:

- Identity Theft Q&A Solution Tree
- LiveChat
- Direct Dialing
- Educational Information
- Resources

The ITRC ID Theft Help Mobile App is available on both the Apple and Android Platforms and is completely free of charge.

www.itrc.org

#IDTheftFTC
Eugenia Buggs
Vice President, Global Marketing, Identity and Digital Protection Services, Generali Global Assistance
Risk is a Reality

• No company or service can guarantee that your identity will never be stolen,

BUT…
Risk is a Reality

• No company or service can guarantee that your identity will never be stolen,

BUT...
There Is

A Lot At Stake

- Loss of Federal or State Benefits
- Inaccurate Medical Treatment
- Loss of Trust
- Denial of Employment
- Having to forego or delay payment of other things
- Damaged Reputation
- Anxiety
- Hassle of having to change banking/credit accounts
- Legal Issues
- Damaged personal relationships
- Financial Loss
- Emotional Distress
- Sense of Frustration
- Loss of Peace of Mind
- Inability to make major purchases
- Invasion of Privacy
- Reduced Credit Score
- Time off or away from work
- An inability to make major purchases
- Invasion of Privacy
Identity Protection Services *Typically Include:*

- Prevention/Education
- **Monitoring & Alerts**
  - Credit
  - Identity
- Resolution
- Insurance
What Should Consumers Research?

• Prevention/Education
  – Trends
  – Tips

ALL SERVICES ARE NOT CREATED EQUAL

• Insurance
  – Is it Insurance
  – What’s Covered

  – 24/7 Availability

#IDTheftFTC
Where Should Consumers Start?

- Financial Institution
- Affinity Organization
- Insurance Company
- Employer
Resources for Recovery
Moderated Discussion
Closing Remarks

Thomas B. Pahl
Acting Director, Bureau of Consumer Protection, Federal Trade Commission
THANK YOU!
Identity Theft

PLANNING FOR THE FUTURE

MAY 24, 2017