Identity Theft & Public Benefits Fraud
IDENTITY THEFT

• **Identity theft** occurs when someone’s Personal Identifying Information (social security number, date of birth, driver’s license information, wage information, medical information, etc.) is accessed/used without his or her knowledge/permission, usually for financial gain.

• **Personal Identifying Information** is being accessed through hacking, theft, negligence, and/or malfeasance by authorized users.
PREVALENCE

• “In 2014 there was a new Identity theft victim every two seconds” – Javelin Strategy and Research 2015

• Identity theft affects everyone (FTC Feb. 2015)

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Prevalence</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-19</td>
<td>6%</td>
</tr>
<tr>
<td>20-29</td>
<td>18%</td>
</tr>
<tr>
<td>30-39</td>
<td>18%</td>
</tr>
<tr>
<td>40-49</td>
<td>19%</td>
</tr>
<tr>
<td>50-59</td>
<td>19%</td>
</tr>
<tr>
<td>60-69</td>
<td>13%</td>
</tr>
<tr>
<td>70+</td>
<td>7%</td>
</tr>
</tbody>
</table>
PREVALENCE

U.S. Population: 320,000,000

Records Breached in 2014: 1,023,108,267

A sampling of populations hit by identity theft in recent years:

- Court Ventures: 200,000,000
- EBay: 145,000,000
- Heartland: 130,000,000
- TJ Maxx: 94,000,000
- AOL: 92,000,000
- Anthem: 80,000,000
- Sony: 77,000,000
- JP Morgan: 76,000,000
- Target: 70,000,000
- Home Depot: 56,000,000
- U.S. OPM: 18,000,000(?)
- Virginia DOH: 8,200,000
- Texas HHS: 2,000,000
- N.D. Univ. Sys: 292,000
- U. Maryland: 287,000
- IRS: 100,000

ID Theft is at crisis levels
What is being done with the hundreds of millions of stolen IDs?

"An estimated $445 billion or 1 percent of the world’s economy was lost due to identity theft or cyber crimes in 2014" – WaPo 2014

- Obtain other identifying information/government documents
- Credit cards, checking, savings – existing
- Credit cards, checking, savings – new
- Utility accounts
- Insurance accounts
- Loans
- Housing rentals
- Car purchases
- Job applications
- Cell phones
- Financial aid
- Medical care
- Firearms purchases
- Tax returns
- Government benefits
Criminals, including organized gangs, are using stolen IDs to steal massive sums from government agencies.

Miami US Attorney: “We are facing a tsunami of fraud. Stolen IDs are the new crack-cocaine of criminal street gangs.”

“Government benefits fraud was the most common form of reported identity theft in 2014” – FTC Feb 2015

“Tax-refund fraud is estimated to reach $21 billion by 2016 due to identity theft” – CNBC Feb 2015
PUBLIC BENEFITS FRAUD

- Criminals are rapidly moving beyond tax fraud to other benefits systems, especially unemployment insurance
- Most agencies are not looking for this type of fraud or don’t know how to look for it
- THIS FRAUD IS PROBABLY HAPPENING IN YOUR SYSTEM
FLORIDA UI EXAMPLE

- **2013**: Identified about 9,600 fraudulent claims through complaints, etc.

- **2014**: Deployed in-house data analytics program and found nearly 70,000 fraudulent claims

- **2015** (as of April 30): Identified 35,000 fraudulent claims (on pace for 100,000 fraudulent claims)

- The potential value of fraudulent claims = $400 million

- **Note**: UI is small in scope (70K claimants) compared to other benefits (3.6M SNAP beneficiaries)
WHY SO MUCH FRAUD?

- Ease of stealing IDs (information is everywhere and unprotected)
- Automation and use of Internet as the primary benefit delivery system
- Mandates for fast payment vs. fraud detection
- Many agencies are not looking for this and are not coordinating
- A safe and profitable crime
  - One claim in all 52 UI programs = $21,000 per week
• Increased staff dedicated solely to ID theft fraud from 6 to 35

• Front-end screening is not particularly effective, and outside companies are not keeping up with this, so we developed an in-house data analytics program

• The technology that enables fraud also has tools to detect fraud and we need to use them

• Fraud Initiative Rating and Rules Engine (FIRRE)

• Platform based on an open-source data analytics software
FLORIDA SOLUTION

• FIRRE looks for patterns that indicate fraud

• Started as a manual process looking intra-day

• Upgraded to automated process looking across timeframes; getting better at catching it earlier

• FIRRE is updated regularly to search for new patterns as criminals adapt to what we shut down

• Pace of identified fraud has not slackened, meaning it’s still profitable and we are not catching it all

• TX and MA saw increased fraud from Florida around the same time we implemented FIRRE
All employees work out of the FIRRE queue on “cases” page.

Claims in FIRRE queue have tripped one of FIRRE’s data trends.

Investigators determine if a claim is to be locked, cleared, or verified.

Obvious id theft is auto locked by the system or locked by investigator.

Obvious legitimate claims are cleared by investigators.

Suspicious claims are sent to verifiers who contact the putative claimant.
“Claim Stats” section displays the number of times IP, email, and bank have been entered into the system over time.

‘FIRRE Report’ section displays ‘trending’ category

Ability to search within individual claim

Additional claimant details

Ability to flag claim for verification, investigation, lock/clear.
Ability to sort/facet into classification for all categories

Search Screen - Provides ability to search by specific criteria.

Additional Categories (e.g. Address, Email, etc.-- 50+)
Faceted IP address view

Clickable link displays IPs in question
User searches for bank account (searchable criteria can be found under ‘advanced search’)

Displays all claims with bank account in question
FLORIDA SOLUTION

• DEO has also revamped its security procedures to protect our data from theft

• E.g.
  • Physical patrols of employee work stations
  • Banning of camera phones near work stations
  • Banning of individual printers
  • Banning of removable storage
  • Review/restriction of access rights
  • Elimination of telecommuting
  • Restructuring of physical space
  • Random audits of computer activity
  • Automated review of computer activity (internal FIRRE)
FLORIDA SOLUTION

Additional Issues

• Inter-agency cooperation
• Funding
• Publicity (fear of; effective use of)
• Balancing payment timeliness
  • E.g., data masking
• Notification to affected parties
• Criminal investigation and prosecution (state/federal)
PRESS

Miami Take Down

Anderson Cooper: Tsunami of Fraud
HOMEWORK

What do public-benefit systems need to think about?

- Is the data you hold adequately protected? 
  NO!

- Are you paying a large amount of fraudulent benefits based on false ID? 
  YES!