Identity Theft and Account Takeover Prevention

Sgt. Rick Radinsky,CFE
520-837-7814

Det. Jeff Van Norman
520-837-7827

Introduction

- Tucson Police Financial Crimes Unit
  - Responsible for investigation of fraud schemes, identity theft, check and credit card forgery, and most other "white-collar" crimes.
  - Composed of 1 Sergeant and 6 Detectives. Receive about 2,400 cases per year, of which slightly less than 10% will be assigned.
- Working Relationships
  - Memberships in IAFCI and ACFE. 3 Certified Fraud Examiners
  - Financial Crimes Task Force
    - Secret Service, USPIS, Marana Police
  - Other local, state and federal agencies

Meet Darryl P.

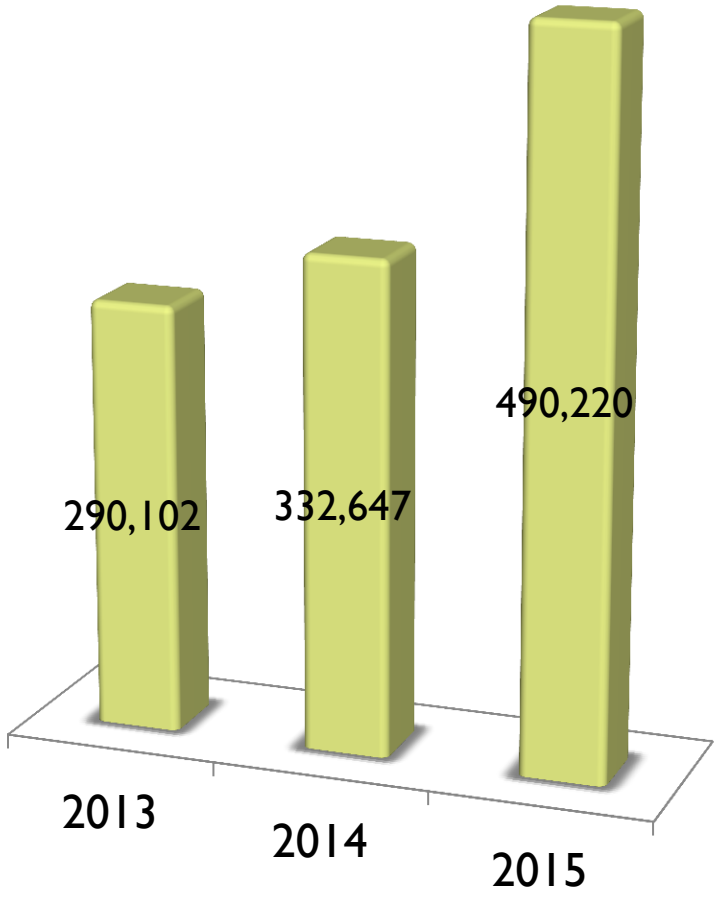
Identity Theft – Definition

- ARS 13-2008: Taking the identity of another person or entity
  - Knowingly
  - Personal Identifying Information (PII) (ARS 13-2001)
    - Name, screen name, signature
    - Driver license, military ID, or social security number
    - Access device or account numbers
    - Birthdate, mother's maiden name, or other info as delineated in the statute
  - For any unlawful purpose or to cause economic loss
  - Class 4 felony
- Most cases that are reported are the use of credit card or bank information.
  - Tax ID theft is on the rise.

Identity Theft Prevalence

Federal Trade Commission Consumer Sentinel Reports

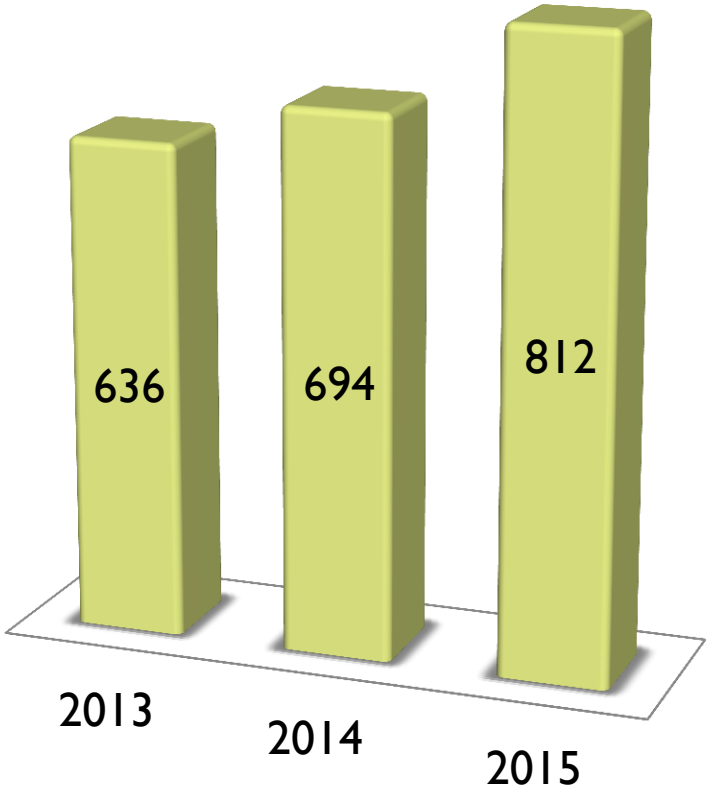
- Increase from 290,102 in 2013 to 490,220 in 2015 (68%)
  - Unrelated factors may have influenced the numbers
    - Amount of feeder agencies reporting may have increased
    - May double count cases (someone reports to feeder agency as well as FTC)



Identity Theft Prevalence

Tucson Police Reports

- Instances reported increased from 636 in 2013 to 812 in 2015 or just over 27%.
- As of 5/19/16, there have been 312 reports generated



How do they get your information?

Technology assisted

- Phishing emails
- Computer spyware/malware
- Internet underground markets
- Hacks of sensitive databases

Old-school

- Dumpster diving
- Theft (purse, wallet, vehicle break-ins)
- Dishonest people with access to records
- Social engineering
- Mail theft

How much data is stolen?

- According to the Identity Theft Resource Center,
  - There were 781 breaches that exposed at least 169 million records in 2015.
    - T-Mobile / Experian
      - 15 million records, including name, address, SSN, DOB, any ID number used to verify identity
    - Scottrade
      - 4.6 million records. Claim only contact info was stolen, though SSN and other data was in same accessed system
    - UCLA Health
      - 4.5 million reocrds. Names, addresses, SSN, and medical data.
    - Army National Guard
      - 850,000 records, including Names, SSN, DOB and home address
- Trend does not appear to be slowing down in 2016

Don’t be an ostrich

Get SHREDded

- From ID Theft Resource Center

Other prevention tips

- Check mail as soon as practical. Do not put outgoing mail in an unsecured mailbox.
- Invest in a crosscut shredder, and use it.
- File your taxes as early in the tax year as practical.
- Sign up for online access to Social Security.
- Keep papers with PII locked up in your home. Do not leave important papers or computers with data on them in your vehicle.

Monitor proactively

- From IdentityTheft.gov:
  - Indicators your info has been stolen
    - Unexplainable bank withdrawls
    - Debt collectors call
    - Unfamiliar accounts on credit reports
    - Insurance shows payment for treatment you never received
    - Letter from IRS that more than one tax return was filed, or you neglected to include income for work you never did
    - Expected mail never arrives
    - Keep computer updated with latest version of operating systems and security patches.
    - Be especially aware when using public computers or Wi-Fi.

Monitoring services

- Things to consider:
  - What information will they be actively monitoring?
  - What services are provided when I become a victim?
  - Are there any financial safety nets (insurance) available in the event I suffer a monetary loss?
  - What's the company's online reviews and BBB standing?
  - What is the cost, and is it worth it for the service that they will provide?
- Basically, it's like any other purchase…do your due diligence.

Identity Theft - Recovery

- Identity theft is a difficult and time consuming crime to recover from. Much of the work must be done by the victim, increasing the level of frustration.
- www.identitytheft.gov
  - Sponsored by the FTC. This site will provide a personalized, step by step recovery plan.
  - For the less internet savvy, copies of the Taking Charge book are available at all Tucson Police substations
    - Monday through Friday 8am-5pm
- Important to follow the steps! This will minimize further damage to your identity, and provide an idea as to how extensive the damage already done is.

Account Takeover Fraud

- Account takeovers occur when someone, committing identity theft, takes control of your financial account(s) for their own purposes.
- Accounts can be taken over by many methods, but almost always due to the compromise of PII
  - Weak or non-existent passwords
  - Phishing emails, phone calls and fake websites
  - Email compromise
  - Social engineering
- When account takeover is successful, anything you could do in your account, the fraudster can do.
  - Transfer money, change billing address, etc.

Account Takeover Prevention

- Password!
  - Should be unique for each financial institution, and associated email addresses
  - Should be **at least** 8 characters, and have mixture of capital letters, numbers and symbols.
  - Words and names should be avoided.
- Two-Factor authentication
  - This should be used whenever available. This provides a text message when an unrecognized computer attempts to sign into your account.

Account Takeover Prevention

- On mobile devices, require a PIN to open your financial account and email apps, if available. Ensure your phone's lockscreen requires a PIN or other type of code to unlock it.
- Apply security updates for both mobile and PCs as soon as practical after they become available.
- Utilize security software to scan for viruses and malware.
- Be skeptical of any emails, texts or phone calls that seek PII and claim to be from a financial institution.

Summary

- All the preventive measures in the world are ineffective if you provide passwords to fraudsters, even if by accident.
- Prevention is much easier, and cheaper, than recovery.
- Take active steps to protect your identity, and monitor it constantly.

Further Resources

- IdentityTheft.gov
  - Federal Trade Commission's official website for victims of identity theft
- ID Theft Resource Center (www.idtheftcenter.org)
  - Wide range of information and assistance available for any and all aspects of identity theft

Contact Information

- Sgt. Rick Radinsky
  - 520-837-7814
  - Rick.Radinsky@TucsonAZ.gov
- Det. Jeff VanNorman
  - 520-837-7827
  - Jeff.VanNorman@TucsonAZ.gov