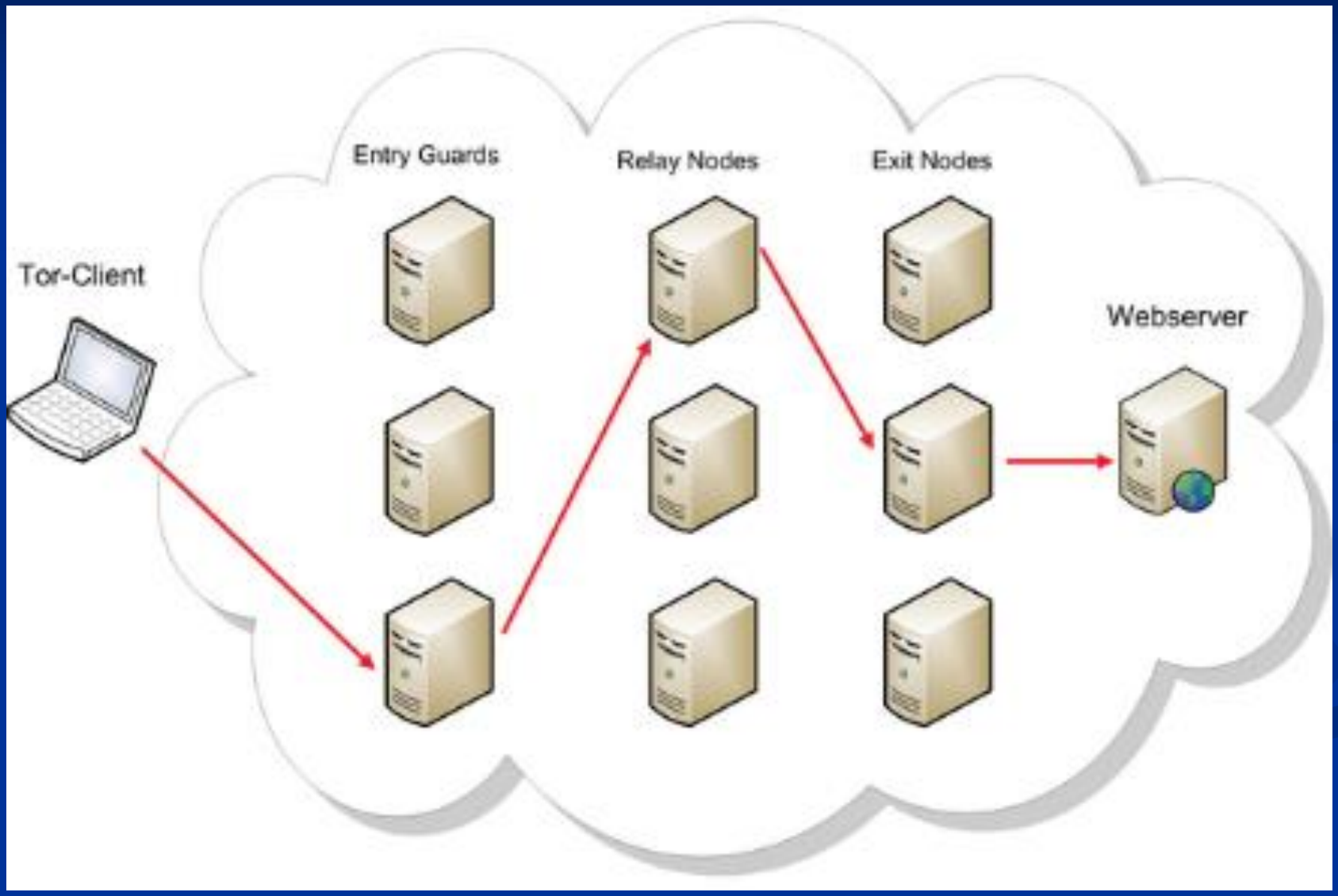
Identity Theft and the Dark Web

Heather Turco
Crime Prevention Specialist
Lee County Sheriff's Office
2020


SURFACE WEB
Google
Wikipedia
Bing
Academic Information
Medical Records
Legal Documents
Scientific Reports
Subscription Information
DEEP WEB
Multilingual Databases
Conference Proceedings
Government Resources
Competitor Websites
Organization-specific Repositories
DARK WEB
Illegal Information
TOR-Encrypted sites
Drug Trafficking sites
Private Communications

Tor-Encrypted Sites



Dark web forums are monitored by the FBI, intelligence agencies, banks and a variety of consultants and specialists who work for corporations. However, there are many forums that frequently move.

Actual case 2019

- The Justice Department shut down a major directory of dark web drug marketplaces and arrested the alleged owners in what federal prosecutors say is a first-of-its-kind operation. It was called the single most significant law enforcement disruption of the Darknet to date.

- The so-called "darknet" or "darkweb" is a part of the internet that can only be accessed by specialized software or hardware and contains websites not found through normal search engines.
- DeepDotWeb was a regular searchable website that provided a directory with direct access to a host of darknet marketplaces selling illegal narcotics including fentanyl, cocaine, heroin and meth.
- The website also provided access to marketplaces for firearms, including assault rifles, and for malicious software and hacking tools.

Alleged owners Tal Prihar, 37, and Michael Phan, 34, both from Israel, were arrested in France and Israel respectively, where they remain in custody. They each face a single count of money laundering conspiracy in the U.S.

- The two allegedly received kickback payments through Bitcoin when someone purchased an item on the darknet sites found through the directory, earning more than $15 million in fees since October 2013.
- These "referral bonuses" allegedly came from darknet marketplaces.
- The closing of DeepDotWeb should stifle hundreds of millions of dollars of illegal purchases.

- The government shut down major darknet drug marketplaces in the past, but they were quickly replaced by new ones.
- In July 2017, federal authorities in the U.S. shut down the AlphaBay and Hansa drug markets.
- But within days another darknet market had already picked up most of the listings, highlighting the challenge authorities face.
- Directories are the way many customers find darknet markeplaces.

The Investigators

- The United States Attorney, French authorities, the United States Postal Inspection Service, Internal Revenue Service, Brazilian Federal Police Cyber Division, Israeli National Police, Dutch National Police, Europol Darkweb Team, Federal Criminal Police Office of Germany, and law enforcement in the United Kingdom. Significant assistance was also provided by the United States Department of Justice, Criminal Division's Office of International Affairs.

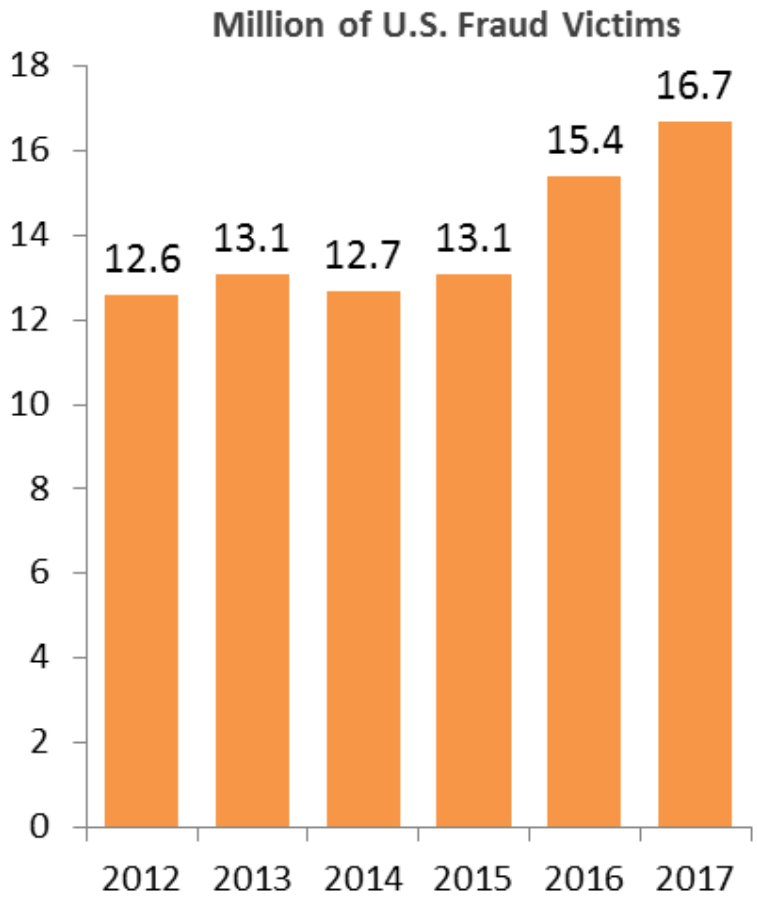
What is Identity Theft?

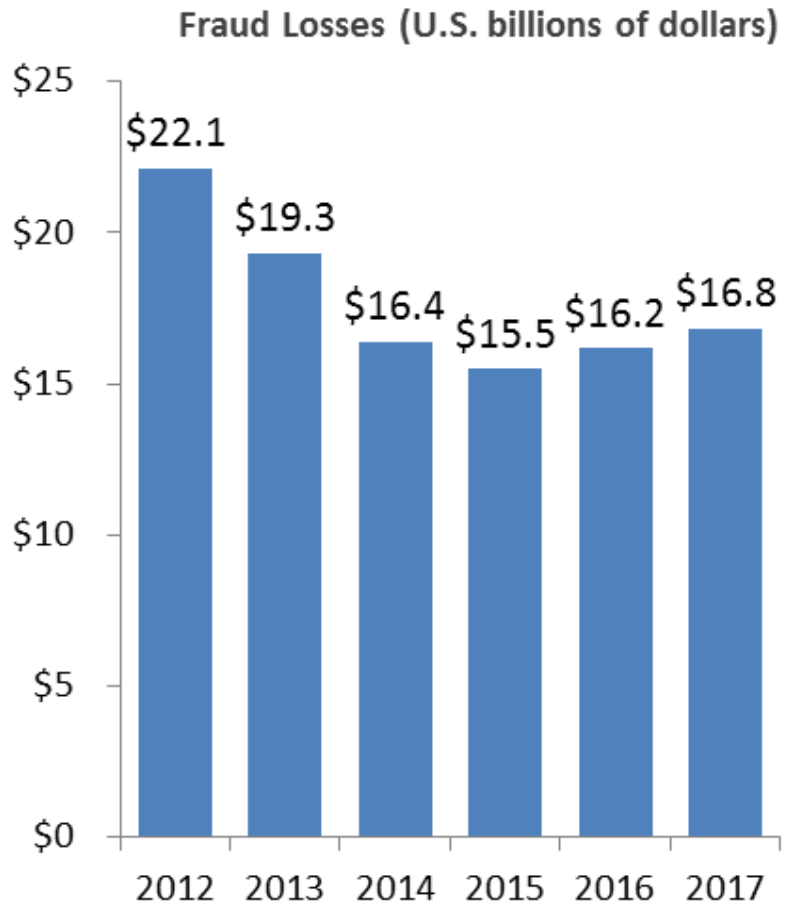
- Identity theft occurs when someone takes your personal information without your knowledge to commit fraud or theft.

Identity theft survey results: Consumers need more education and help. Most Americans are unwitting accomplices to their own identity theft.

News of data breaches and the risks of identity theft and fraud continue to grow but consumers' vigilance and awareness haven't kept pace.

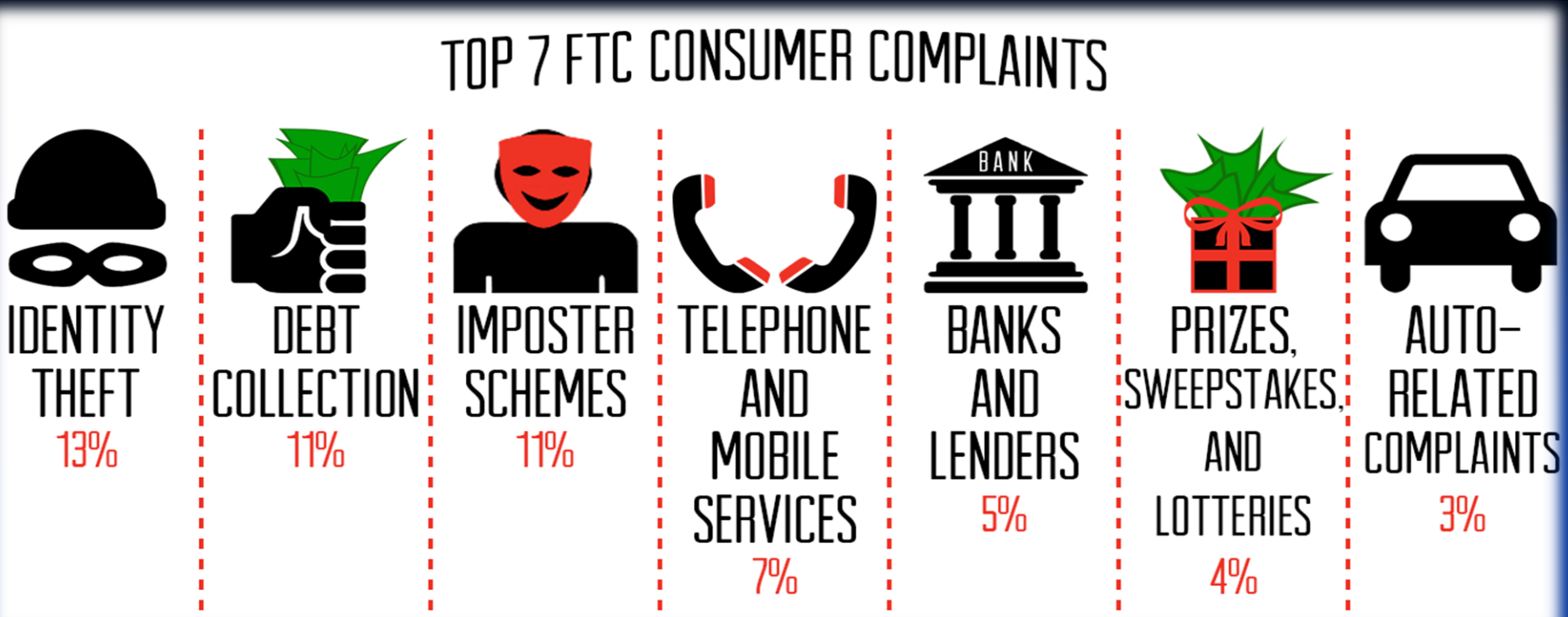
Fraud Victims and Losses Continue Three-Year Rise





Source: *2018 Identity Fraud Study*, Javelin Strategy & Research

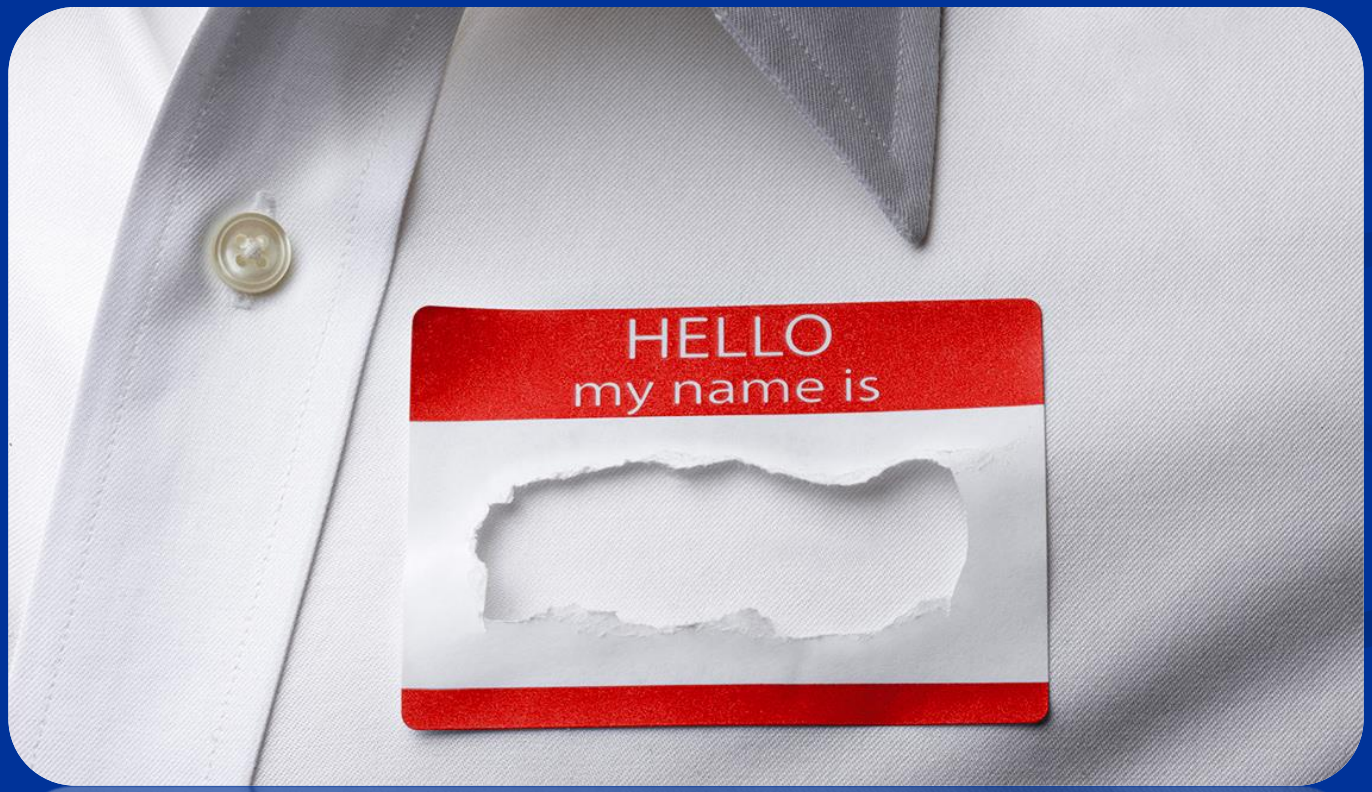
JAVELIN



Identity Theft is the #1 complaint.

FLORIDA #2
FOR IDENTITY THEFT

An Identity is Stolen every 2 SECONDS in the U.S.



Types of Identity Theft

- Financial
- Medical
- Social Security
- Tax-Related

Types of Identity Theft

- Driver License
- Child
- Deceased
- Synthetic

Ways Your ID is Stolen

- Credit card theft - Your credit card passes through countless hands and offers many opportunities for a thief to steal your credit card number. If possible, swipe/insert your own card, and don't let your card out of your sight.

Ways Your ID is Stolen

- Unsecured Websites - Before you make your next online purchase, make sure the website is secure. If the URL starts with "https," then you should be safe.

Ways Your ID is Stolen

- Phishing - an email-based scam in which a thief poses as a real organization, agency or company. The email prompts you to enter personal information. If something seems strange or the message requests too much private data, don't click on the links.

Ways Your ID is Stolen

- Hacking - Thieves hack into a variety of computer systems, from banks to retail chains, to steal credit card and bank information. Most organizations alert their customers to a security breach as soon as possible. If you receive this type of message, though, confirm whether your data has been compromised and then take steps to close your credit card if necessary.

Actual Case

- On September 14, 2019, LCSO received a call for service in Fort Myers in reference to an identity theft.
- The victim stated the following: a Hispanic male and female from a company identified as "Aquafeel" arrived at her residence to check her water system.
- They suggested that she needed to buy a potable water treatment system.
- The victim then completed an application and supplied all of her personal information, including her social security number.

- After filling out the application, the two left and stated they would return Monday.
- Approximately 5 hours after they left, the victim received a phone call from Fucillo Kia Cape Coral, advising that an unidentified person submitted an application online to purchase a vehicle, with the victim's personal information.

- The victim explained she submitted no application.
- It should be noted the victim took a picture of the females' driver's license.
- LCSO conducted a search of the driver's license, and confirmed the license was valid.

Passwords


PASSWORDS ARE LIKE
UNDERPANTS
Change them often, keep them private and never share them with anyone.

Ways Your ID is Stolen

- Shoulder Surfing – Cover your screen with your hand as you enter personal data in a public setting.

Ways Your ID is Stolen

- Skimming - An identity thief installs an additional device onto an existing ATM or credit card reader. This device can read your credit card information, including your ATM or debit card PIN. If you notice an oddly shaped credit card reader, or there's a noticeable difference in your regular ATM reader, notify the owner and don't use the machine.

Ways Your ID is Stolen

- Pretexting - Thieves call banks, utility companies or other organizations and use false pretenses to steal your personal information. If you see new account activity that you haven't initiated, contact the institution right away.

Ways Your ID is Stolen

- Dumpster Diving - When thieves go through your discarded trash in search of bank statements or credit card information. Shred your statements.
- Mail theft - Some thieves cut right to the chase and steal your statements or new credit cards directly from your mailbox.

Employee Thieves

- Personal information can be stolen and sold by an employee who works or pretends to work for a:
  - Medical Facility
  - Home Health Agency
  - Billing Agency
  - Document Shredder
  - Bank/Credit Card Company
  - Tax Preparer

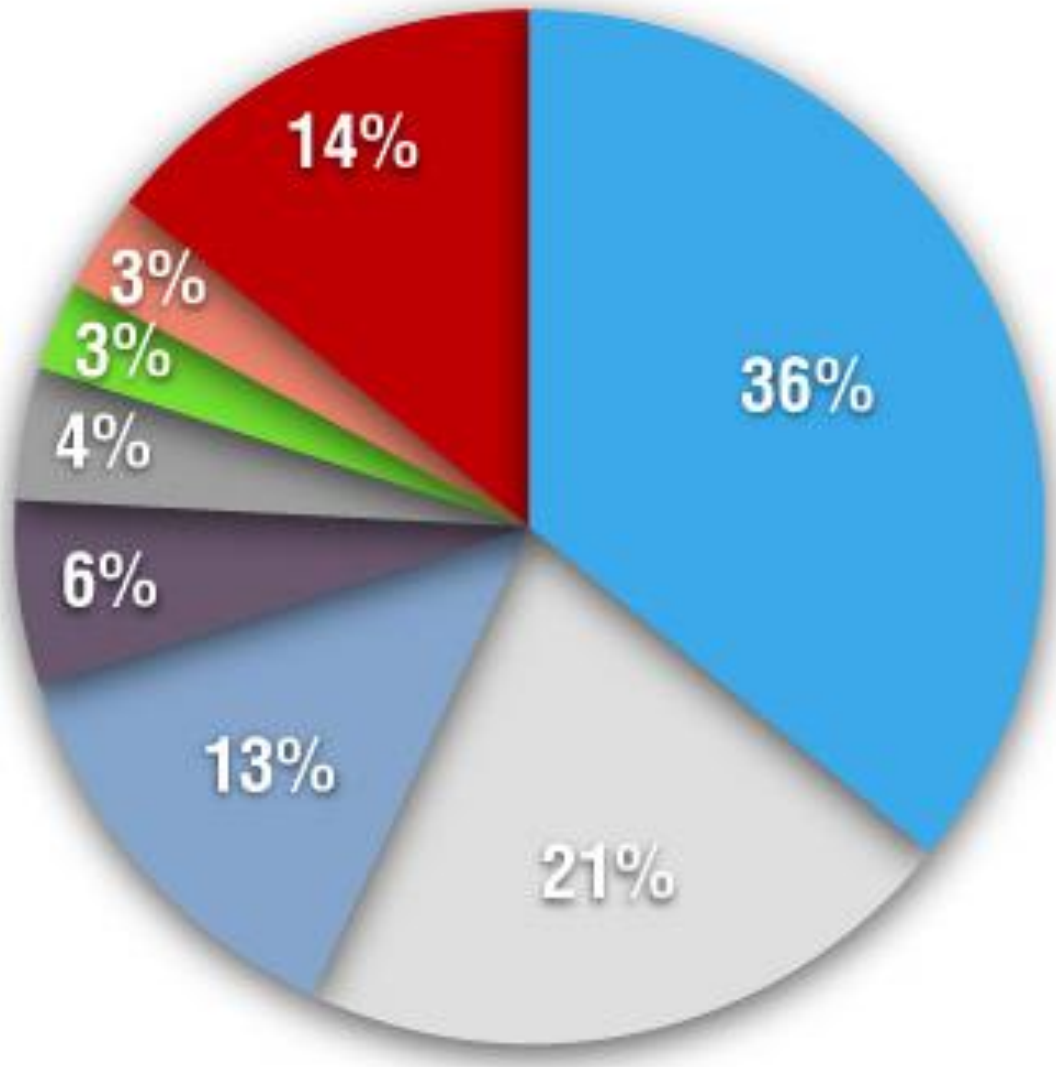
Actual Case

- On 9/20/19, victim contacted LCSO to report an identity theft.
- The victim advised on 9/12/19 she received a phone call from Alamo in reference to a vehicle rented on 9/3/19 with her personal information which was supposed to be returned on 9/5/19, but never was.

Actual Case

- The victim advised on 9/13/19 she received a letter from Avis in reference to a vehicle rented on 8/4/19 with her personal information which was supposed to be returned on 8/11/19, but never was.
- The victim did not rent these 2 vehicles, nor did she allow anyone to use her identity for any reason.

What thieves do once they steal your info



- Use existing credit or debit card
- Commit tax or employment fraud
- Obtain new credit card
- Obtain medical/Social Security benefits
- Utilities (Including buying, reselling phones)
- Open a new bank account, line of credit
- Get a car loan
- Other

Source: Travelers

CreditCards.com

On the Dark Web

Criminal Details

Employment- or tax-related fraud (34%)

- A criminal uses someone else's Social Security number and other personal information to gain employment or to file an income tax return.

Credit card fraud (33%)

- The thief uses someone else's credit card or credit card number to make fraudulent purchases.

Criminal Details

~ Phone or utilities fraud (13%)

- The criminal uses another person's personal information to open a wireless phone or utility account.

~ Bank fraud (12%)

- The fraudster uses someone else's personal information to take over an existing financial account or to open a new account in another's name.

Criminal Details

~ Loan or lease fraud (7%)

- A borrower or lessee uses another's information to obtain the loan or lease.

~ Government documents or benefits fraud (7%)

- The criminal uses stolen personal information to obtain government benefits.

Guard Your Personal Information

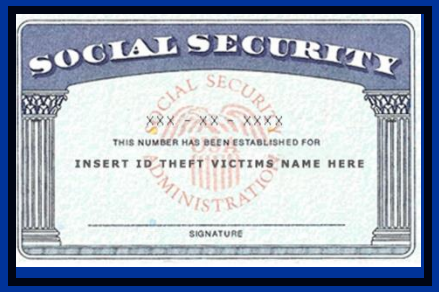
~ Credit card number

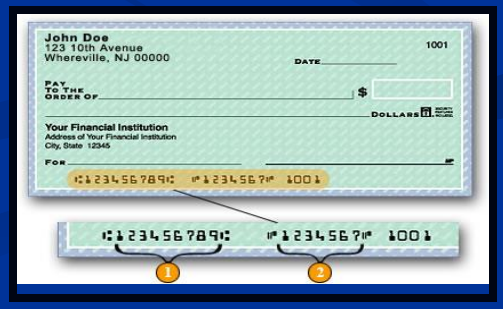
~ Driver license number

~ Bank account number

~ Social Security number

~ Date of Birth





Who's calling and Why?

DO NOT ANSWER!

- Let the caller leave a voice message.
- You can decide if you want to call them back.
- If no message is left, do not call number back.

HANG UP!

What about mail?

Take bill payments to post office instead of putting in mailbox with **RED** flag up.

Quote from a Identity Thief

"I'd find people who are hard-up for money," he said. "They're not real criminals. Or they don't consider stealing out of mailboxes makes them a criminal. So I would give them $400-$500 and they'd steal me trash bags full of mail. And I'd even give them a car to do it in, usually a rental car I got with a stolen identity and never gave back. It's just so easy with mail theft. You don't have to be a hacker. You don't have to talk to anybody, you don't have to trick anybody, you know what I mean? You just open a mailbox."

Synthetic Identity


ISSUED: 07-05-2013
EXPIRES: 03-05-2013
SEX: A
ENDORSE
SAFE DRIVER
Florida
Bank of America
Platinum Card
VISA

Identity Theft After Death

Every year **2.5 million** deceased Americans have their identity stolen.

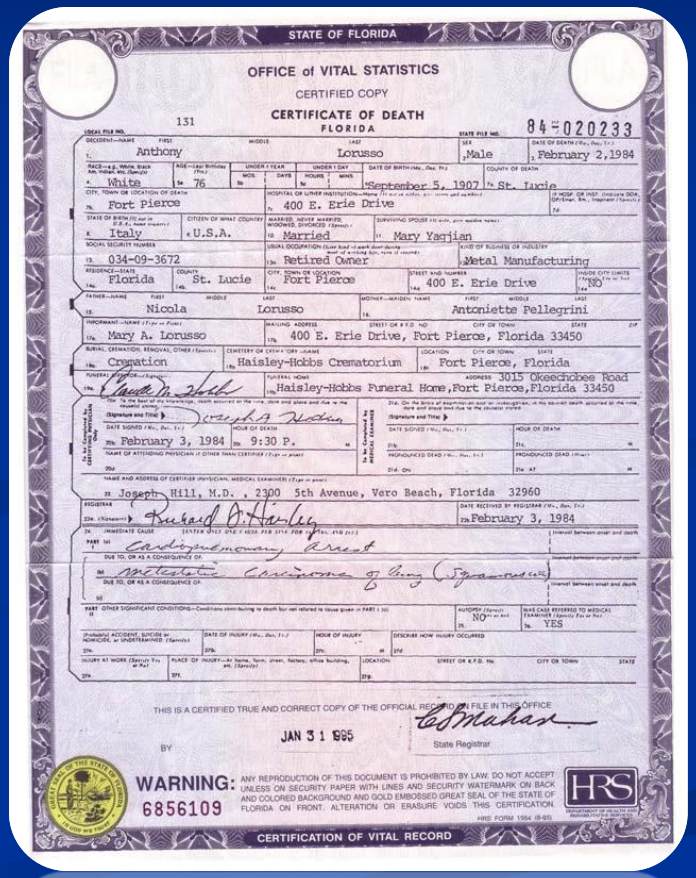

FOX 17
NEWS AT TEN
SKY ARNOLD
@SKYARNOLD1

Why Target the Deceased?

- **Someone** wants a fresh start in life and could actually acquire and maintain the good credit history of the deceased.
- It can take **six months** for death records to be registered or shared by financial institutions, credit bureaus, and the Social Security Administration.
- The dead are unable to monitor their credit — and often, neither do their grieving survivors.

How to prevent ID theft of the Deceased

- Stop the mail.
- Close accounts.
- Monitor credit.
- Notify creditors.
- Avoid long obituaries.
- Close social media accounts.



STATE OF FLORIDA

OFFICE of VITAL STATISTICS

CERTIFIED COPY

CERTIFICATE OF DEATH

FLORIDA

131

84-020233

Anthony | Lorusso | Male | February 2,1984

White | 76 | September 5, 1907 | St. Lucie

Fort Pierce | 400 E. Erie Drive

Italy | U.S.A. | Married | Mary Yagjian

034-09-3672 | Retired Owner | Metal Manufacturing

Florida | St. Lucie | Fort Pierce | 400 E. Erie Drive | NO

Nicola | Lorusso | Antoniette Pellegrini

Mary A. Lorusso | 400 E. Erie Drive, Fort Pierce, Florida 33450

Cremation | Haisley-Hobbs Crematorium | Fort Pierce, Florida

Haisley-Hobbs Funeral Home, Fort Pierce, Florida 33450 | 3015 Okeechobee Road

February 3, 1984 | 9:30 P.

Joseph Hill, M.D., 2300 5th Avenue, Vero Beach, Florida 32960

February 3, 1984

Cardiopulmonary Arrest

Metastatic Carcinoma of Lung (Squamous)

NO | YES

THIS IS A CERTIFIED TRUE AND CORRECT COPY OF THE OFFICIAL RECORD ON FILE IN THIS OFFICE

JAN 31 1995

State Registrar

WARNING: ANY REPRODUCTION OF THIS DOCUMENT IS PROHIBITED BY LAW. DO NOT ACCEPT UNLESS ON SECURITY PAPER WITH LINES AND SECURITY WATERMARK ON BACK AND COLORED BACKGROUND AND GOLD EMBOSSED GREAT SEAL OF THE STATE OF FLORIDA ON FRONT. ALTERATION OR ERASURE VOIDS THIS CERTIFICATION.

6856109

HRS

CERTIFICATION OF VITAL RECORD

What Else Can You Do?

Place "**deceased alert**" on credit reports

Contact:
DMV, SSA, Memberships

Beware of **scams**

Debt Collector
IRS Imposter
Fee to Release Records
You Were Left Money
Long Lost Relatives

facebook

Close social media accounts

Obituary

- Use age instead of Date of Birth
- Less information. Shorter is better.
- Omit middle name and home address.
- Leave out mother's maiden name.

The Memorial

- Be wary of funeral / burial scams – phishing.
- Have a house-sitter for service or memorial. Burglars target empty houses during services.
- Use phone number for more information, not date/time.

What is Medical ID Theft?

- When someone uses your personal information such as name, DOB, insurance, SSN, driver license to obtain **medical** services or goods.

How Big is the Problem?

- **91%** of health organizations have had a data breach in past 2 years. (MIFA)
- Last 5 years over 120,000 data breaches of personal medical information of over **31 million** people (US Dept of Health & Human Services)
- **2.3 million** people are victims. Increase of 22% (Medical Identity Theft Alliance)

Why Does it Happen?

- Personal ID passes through many hands at medical facilities.
- More information in a medical record than a bank/credit card or DL.
- Medical information sells for more money than other personal information.

Why Does it Happen?

- Patient files identified by SSN's.
- Patient forms provide blanks that are filled in by new patients without asking if necessary.

The Dangers of Medical ID Theft

~ Denied treatment or misdiagnosed based on inaccurate information.

~ Denied life insurance or billed for services not rendered.

~ Denied records under HIPAA since your info is intermingled with someone else's.

~ Can be life-threatening.

Signs of Medical ID Theft

- A bill for services not received
- A call from debt collector for services not received
- Medical collection notices on your credit report

Signs of Medical ID Theft

- A notice from your health plan that you reached your benefit limit
- Denial of insurance for medical condition, you do not have

Protect Against Medical ID Theft

- Check medical records annually
- Read insurance benefit notices carefully
- Replace lost insurance card with new ID

Reducing Your Overall Risk of ID Theft

- What's in your…
  - wallet?
  - mailbox?
  - credit reports?
  - email?
  - trash?

Reducing Your Overall Risk of ID Theft

- What's on your…
  - computer?
  - social media?
  - desk?
  - lips?

Reduce Your Risk of SSN Redirection

- Go to www.ssa.gov
- Follow instructions to create user name and password
- Answer security questions
- Give social security number

Victim Assistance

Victim: 7 year alert
Non victim: 90 days
Contact one credit bureau
Law requires them to share your request

Credit Freeze

- ✓Contact credit bureaus
- ✓Receive PIN
- ✓Free

Remember the 3 C's

- **Check**: Look through all your financial, professional and personal accounts to see if anything is out of the ordinary and change passwords. Contact banks to alert them, cancel cards and have them replaced.

- **Contact**: File a report with the Federal Trade Commission, the Internet Crime Complaint Center and local law enforcement.

- **Collect**: Collect any and all evidence you may have to support your claim. This could be cancelled checks, credit card receipts, unusual social media or email messages, etc.

Source: Florida Department of Financial Regulation

Identity Theft and the Dark Web

Heather Turco
Crime Prevention Specialist
Lee County Sheriff's Office

2020