Identity Theft
How to Avoid it

A Presentation for

STUG

Wednesday January 4, 2017

Hewie Poplock

hewie@hewie.net

What is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number, etc., in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud, which may include:

- Taking over the victim's financial accounts or obtaining fraudulent financial accounts;
- Making purchases in the victim's name;
- Applying for loans, credit cards, social security benefits, etc.;
- Establishing services with utility and phone companies.

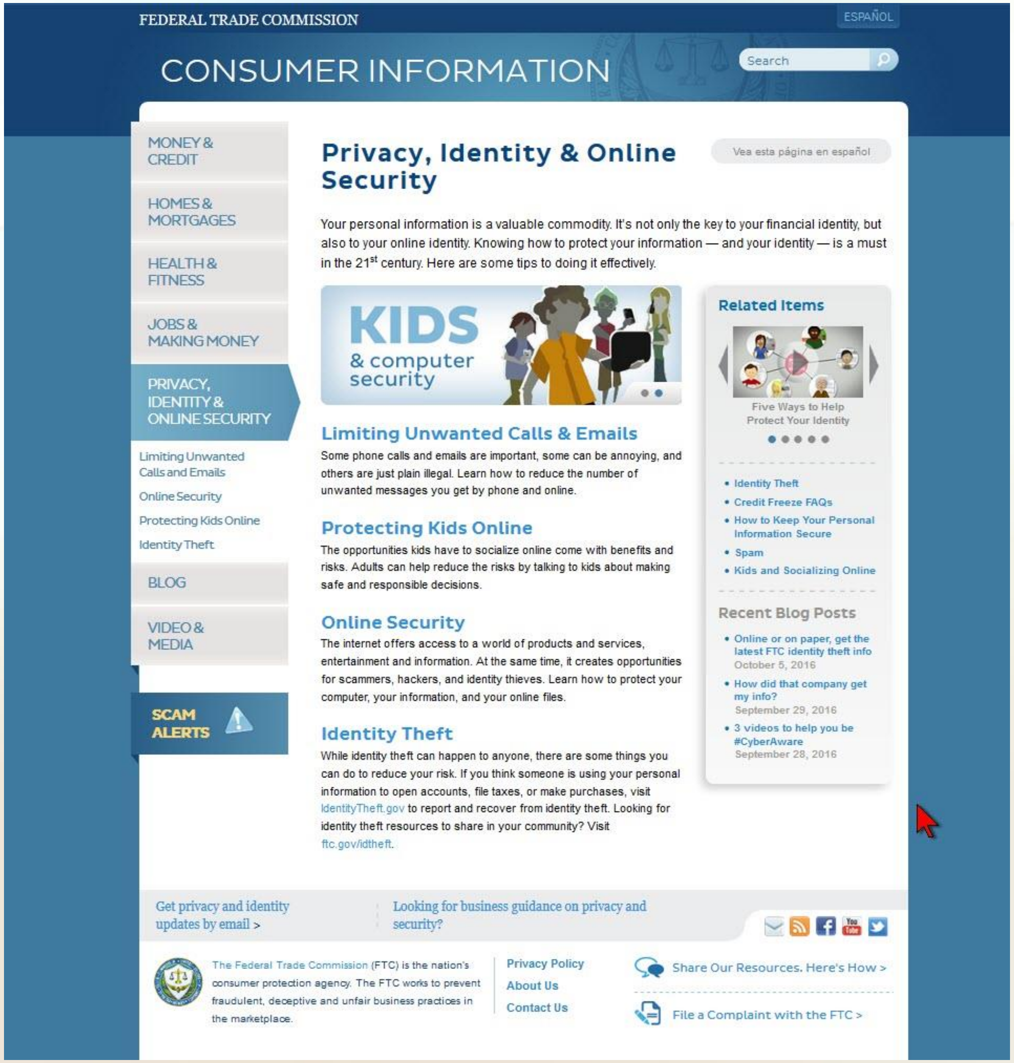
Identity theft may be used to facilitate crimes including illegal immigration, terrorism, and espionage. Identity theft may also be a means of blackmail. There are also cases of identity cloning to attack payment systems, including medical insurance.

Common Types of ID Theft

- Child ID Theft - Children’s IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.
- Tax ID Theft - A thief uses your social security number to falsely file tax returns with the Internal Revenue Service or state government.
- Medical ID Theft - This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.
- Senior ID theft - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.
- Social ID theft - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

https://www.usa.gov/identity-theft

Federal Trade Commission Website



FEDERAL TRADE COMMISSION

ESPAÑOL

CONSUMER INFORMATION

Search

- MONEY & CREDIT
- HOMES & MORTGAGES
- HEALTH & FITNESS
- JOBS & MAKING MONEY
- PRIVACY, IDENTITY & ONLINE SECURITY
  - Limiting Unwanted Calls and Emails
  - Online Security
  - Protecting Kids Online
  - Identity Theft
- BLOG
- VIDEO & MEDIA

SCAM ALERTS

Privacy, Identity & Online Security

Vea esta página en español

Your personal information is a valuable commodity. It's not only the key to your financial identity, but also to your online identity. Knowing how to protect your information — and your identity — is a must in the 21st century. Here are some tips to doing it effectively.

KIDS & computer security

Limiting Unwanted Calls & Emails

Some phone calls and emails are important, some can be annoying, and others are just plain illegal. Learn how to reduce the number of unwanted messages you get by phone and online.

Protecting Kids Online

The opportunities kids have to socialize online come with benefits and risks. Adults can help reduce the risks by talking to kids about making safe and responsible decisions.

Online Security

The internet offers access to a world of products and services, entertainment and information. At the same time, it creates opportunities for scammers, hackers, and identity thieves. Learn how to protect your computer, your information, and your online files.

Identity Theft

While identity theft can happen to anyone, there are some things you can do to reduce your risk. If you think someone is using your personal information to open accounts, file taxes, or make purchases, visit IdentityTheft.gov to report and recover from identity theft. Looking for identity theft resources to share in your community? Visit ftc.gov/idtheft.

Related Items

Five Ways to Help Protect Your Identity

- Identity Theft
- Credit Freeze FAQs
- How to Keep Your Personal Information Secure
- Spam
- Kids and Socializing Online

Recent Blog Posts

- Online or on paper, get the latest FTC identity theft info
  October 5, 2016
- How did that company get my info?
  September 29, 2016
- 3 videos to help you be #CyberAware
  September 28, 2016

Get privacy and identity updates by email >

Looking for business guidance on privacy and security?

The Federal Trade Commission (FTC) is the nation's consumer protection agency. The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace.

Privacy Policy
About Us
Contact Us

Share Our Resources. Here's How >

File a Complaint with the FTC >

http://www.consumer.ftc.gov/topics/privacy-identity

Ways Identity Theft Can Occur

Thieves:

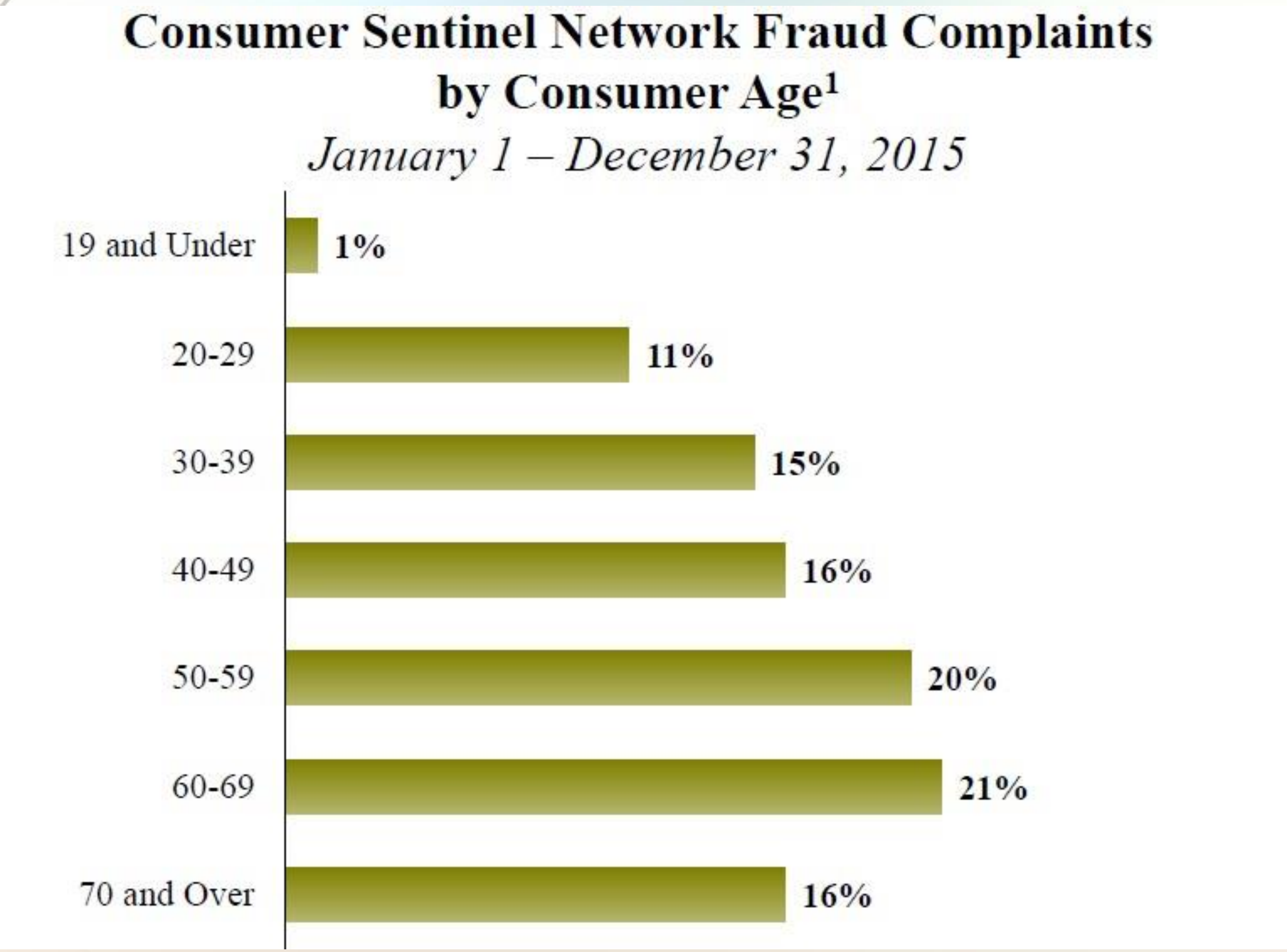
- Steal wallets and purses containing personal identification and credit/bank cards or items with your Social Security Number. Purse Snatching & Pick Pockets.
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks and tax information
- Watching you writing checks and/or checking your mail box.
- Complete a change of address form to divert mail to another location.
- Rummage through trash, or the trash of businesses, for personal data in a practice known as “dumpster diving”
- Find personal information in homes
- Use personal information individuals share on the Internet
- Credit Card Skimming

Ways Identity Theft Can Occur

Thieves (continued):

- Send e-mail posing as legitimate companies or government agencies with which individuals do business. (phishing)
- Get information from the workplace in a practice known as “business record theft” by stealing files out of offices where a person is a customer, employee, patient or student, bribing an employee who has access to personal files, or “hacking” into electronic files.
- Eavesdrop on public transactions to obtain personal data (shoulder surfing)
- Drive by (pharming)
- Browse social network (Facebook, Twitter, Other Social Networking, etc.) sites, online for personal details that have been posted by users
- Simply research about the victim in government registers, at the Internet, Google, etc.

ID Theft by Age 2015

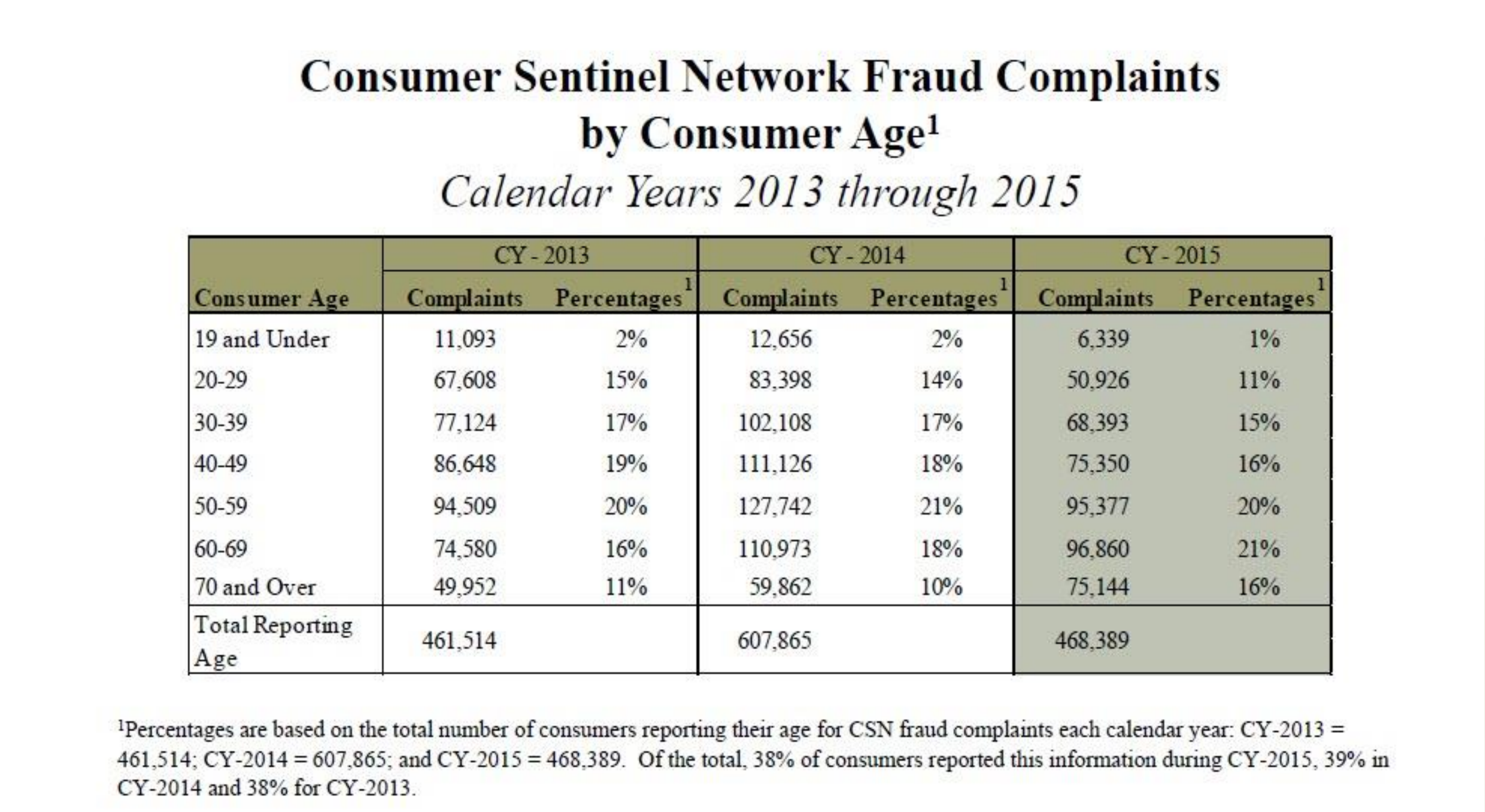


Consumer Sentinel Network Fraud Complaints by Consumer Age[1]

January 1 – December 31, 2015

Consumer Sentinel Network Data Book for January - December 2015
Federal Trade Commission Released February 2016

ID Theft by Age 2013-2015



Consumer Sentinel Network Fraud Complaints by Consumer Age[1]

Calendar Years 2013 through 2015

	CY - 2013		CY - 2014		CY - 2015	
Consumer Age	Complaints	Percentages[1]	Complaints	Percentages[1]	Complaints	Percentages[1]
19 and Under	11,093	2%	12,656	2%	6,339	1%
20-29	67,608	15%	83,398	14%	50,926	11%
30-39	77,124	17%	102,108	17%	68,393	15%
40-49	86,648	19%	111,126	18%	75,350	16%
50-59	94,509	20%	127,742	21%	95,377	20%
60-69	74,580	16%	110,973	18%	96,860	21%
70 and Over	49,952	11%	59,862	10%	75,144	16%
Total Reporting Age	461,514		607,865		468,389	

[1] Percentages are based on the total number of consumers reporting their age for CSN fraud complaints each calendar year: CY-2013 = 461,514; CY-2014 = 607,865; and CY-2015 = 468,389. Of the total, 38% of consumers reported this information during CY-2015, 39% in CY-2014 and 38% for CY-2013.

Consumer Sentinel Network Data Book for January - December 2015
Federal Trade Commission Released February 2016

5 Groups At Greater Risk Of Identity Theft

- Social media users a growing target
- Paying with plastic makes you vulnerable
- Mobile phone users a new target
- Children aren't immune
- Executives are a rich target

http://www.bankrate.com/finance/credit/groups-greater-risk-identity-theft.aspx

2_min41sec_5ways_to_steal_id

Help Protect Yourself

American consumers' data has been exposed with such frequency that about 1 in 6 adults say they or someone they know is a victim of identity theft, according to Bankrate's latest Money Pulse survey.

You aren't in total control when it comes to your data, but there are things you can do to protect yourself. Start by avoiding these 6 bad habits.

"It's definitely worth being worried about protecting yourself," says Tim Erlin, director of IT security and risk strategy at Tripwire, a cyber-security firm. "As a consumer, you can't be worried necessarily which company will be compromised next."

Protect Yourself

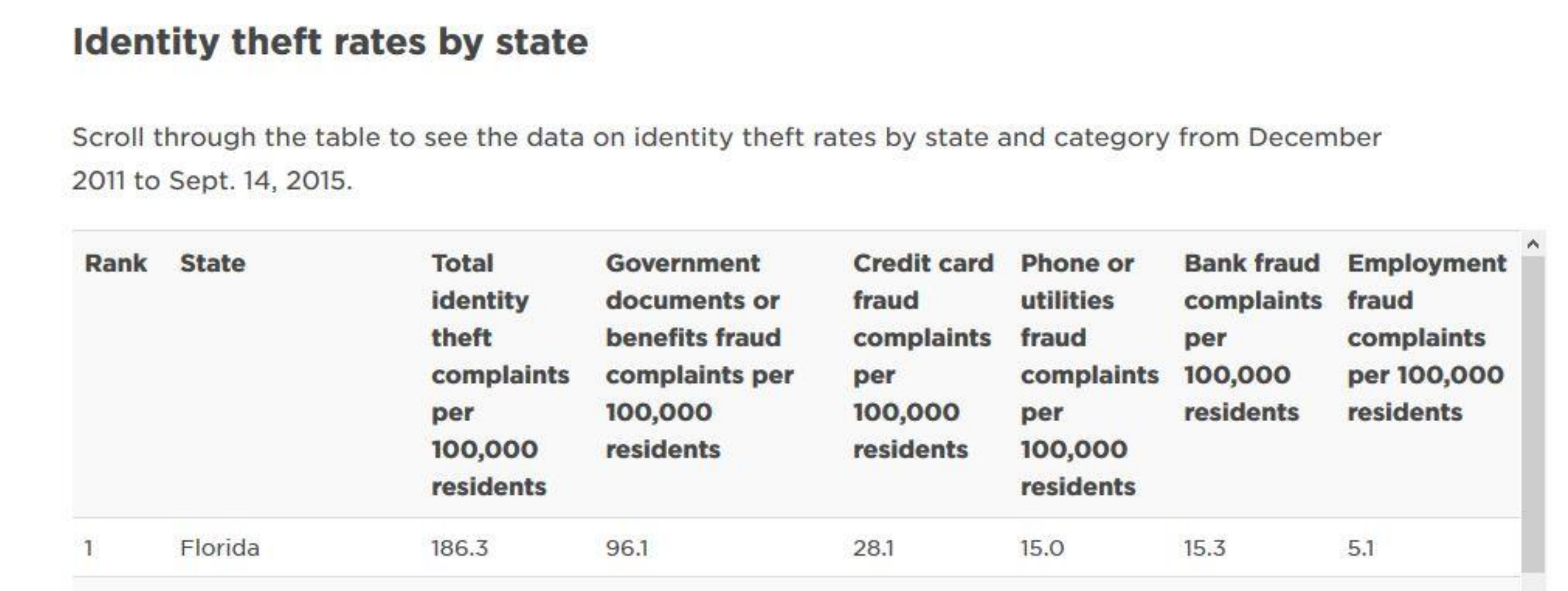
6 bad habits that help ID thieves get your data

- Tossing sensitive documents into the trash
- Failing to check credit reports
- Banking on unsecured Wi-Fi
- Using the same password across multiple accounts
- Failing to monitor accounts
- Failing to freeze your credit after a breach

Florida Ranks 1st In U.S. For ID Theft

Florida is 1st

Florida is No. 1. The Sunshine State leads the way in overall identity theft complaints per capita, with 186 per 100,000 residents. Washington, Washington, D.C., Oregon and Missouri also have higher rates of identity theft. Meanwhile, the lowest rate of identity theft complaints was in South Dakota, Hawaii and North Dakota. In comparison, data show that per capita, there were nearly five times as many identity theft complaints in Florida as in Hawaii.



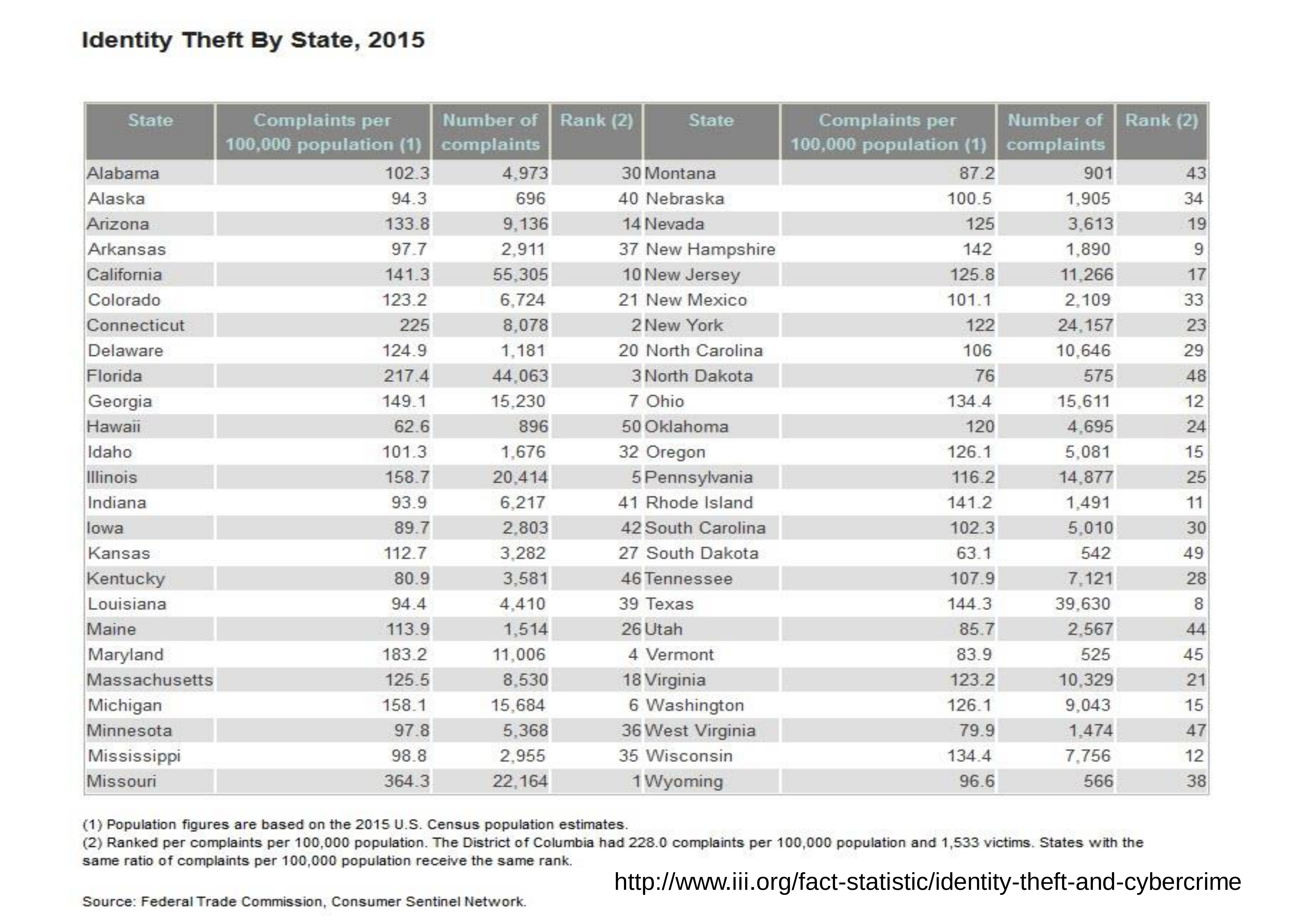
Identity theft rates by state

Scroll through the table to see the data on identity theft rates by state and category from December 2011 to Sept. 14, 2015.

Rank	State	Total identity theft complaints per 100,000 residents	Government documents or benefits fraud complaints per 100,000 residents	Credit card fraud complaints per 100,000 residents	Phone or utilities fraud complaints per 100,000 residents	Bank fraud complaints per 100,000 residents	Employment fraud complaints per 100,000 residents
1	Florida	186.3	96.1	28.1	15.0	15.3	5.1

https://www.nerdwallet.com/blog/credit-card-data/identity-theft-credit-card-fraud-2015/

Identity Theft by State 2015



Identity Theft By State, 2015

State	Complaints per 100,000 population (1)	Number of complaints	Rank (2)	State	Complaints per 100,000 population (1)	Number of complaints	Rank (2)
Alabama	102.3	4,973	30	Montana	87.2	901	43
Alaska	94.3	696	40	Nebraska	100.5	1,905	34
Arizona	133.8	9,136	14	Nevada	125	3,613	19
Arkansas	97.7	2,911	37	New Hampshire	142	1,890	9
California	141.3	55,305	10	New Jersey	125.8	11,266	17
Colorado	123.2	6,724	21	New Mexico	101.1	2,109	33
Connecticut	225	8,078	2	New York	122	24,157	23
Delaware	124.9	1,181	20	North Carolina	106	10,646	29
Florida	217.4	44,063	3	North Dakota	76	575	48
Georgia	149.1	15,230	7	Ohio	134.4	15,611	12
Hawaii	62.6	896	50	Oklahoma	120	4,695	24
Idaho	101.3	1,676	32	Oregon	126.1	5,081	15
Illinois	158.7	20,414	5	Pennsylvania	116.2	14,877	25
Indiana	93.9	6,217	41	Rhode Island	141.2	1,491	11
Iowa	89.7	2,803	42	South Carolina	102.3	5,010	30
Kansas	112.7	3,282	27	South Dakota	63.1	542	49
Kentucky	80.9	3,581	46	Tennessee	107.9	7,121	28
Louisiana	94.4	4,410	39	Texas	144.3	39,630	8
Maine	113.9	1,514	26	Utah	85.7	2,567	44
Maryland	183.2	11,006	4	Vermont	83.9	525	45
Massachusetts	125.5	8,530	18	Virginia	123.2	10,329	21
Michigan	158.1	15,684	6	Washington	126.1	9,043	15
Minnesota	97.8	5,368	36	West Virginia	79.9	1,474	47
Mississippi	98.8	2,955	35	Wisconsin	134.4	7,756	12
Missouri	364.3	22,164	1	Wyoming	96.6	566	38

(1) Population figures are based on the 2015 U.S. Census population estimates.

(2) Ranked per complaints per 100,000 population. The District of Columbia had 228.0 complaints per 100,000 population and 1,533 victims. States with the same ratio of complaints per 100,000 population receive the same rank.

Source: Federal Trade Commission, Consumer Sentinel Network.

http://www.iii.org/fact-statistic/identity-theft-and-cybercrime

Phishing

Definition: Brand Spoofing is a scam in which perpetrators disguise themselves as well-known companies and “phish” for personal information.

What are Identity Thieves Looking For?

- **Social Security Numbers**
- **Date of Birth**
- **Passwords or Personal Identification Numbers (PINS)**
- **Account Numbers (credit card, bank)**
- **ATM/Debit Card Number**

Phishing

When internet fraudsters impersonate a business to trick you into giving out your personal information, it’s called phishing. Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don’t click on links within them either – even if the message seems to be from an organization you trust. It isn’t. Legitimate businesses don’t ask you to send sensitive information through insecure channels.

https://www.consumer.ftc.gov/articles/0003-phishing

Examples of Phishing Messages

You open an email or text, and see a message like this:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
- “Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund.”

The senders are phishing for your information so they can use it to commit fraud.

https://www.consumer.ftc.gov/articles/0003-phishing

How to Deal with Phishing Scams

- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text.
- The messages may appear to be from organizations you do business with – banks, for example. They might threaten to close your account or take other action if you don’t respond.
- Don’t reply, and don’t click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.
- Area codes can mislead, too. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn’t guarantee that the caller is local.
- If you’re concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

https://www.consumer.ftc.gov/articles/0003-phishing

Steps To Avoid A Phishing Attack

- Use trusted security software and set it to update automatically. In addition, use these computer security practices.
- Don't email personal or financial information. Email is not a secure method of transmitting personal information.
- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.

https://www.consumer.ftc.gov/articles/0003-phishing

Report Phishing Emails

- Forward phishing emails to spam@uce.gov — and to the company, bank, or organization impersonated in the email. Your report is most effective when you include the full email header, but most email programs hide this information. To find out how to include it, type the name of your email service with “full email header” into your favorite search engine.
- You also can report phishing email to reportphishing@antiphishing.org. The Anti-Phishing Working Group — which includes ISPs, security vendors, financial institutions and law enforcement agencies — uses these reports to fight phishing.

If you might have been tricked by a phishing email:

- File a report with the Federal Trade Commission at www.ftc.gov/complaint.
- Visit the FTC’s Identity Theft website. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

https://www.consumer.ftc.gov/articles/0003-phishing

13_sec_ShoppingCart purse-snatching

2_min_8sec_Police searching for Altamonte Springs purse snatcher www-wftv-com

Yahoo Data Breach

The Yahoo Data Breach May Be Biggest Breach in History

There was a time when hackers sought out retailers’ computer networks, specifically their point-of-sale credit card networks, and used that access to steal credit card and debit card information. Over time, there’s been a shift in the way hackers operate.

After all, stealing your credit card information is a very limited prospect; all you have to do is cancel that card when you notice some suspicious activity, and their efforts will prove fruitless. That’s why hackers have upped their game, going after long-standing information and personal data rather than account numbers that can be changed. The most recent large scale data breach, one that affected more than 1 billion accounts, proves that very point.

Several sources have now reported that Yahoo! has experienced a data breach, believed to be the work of foreign, state-sponsored hackers. The sheer volume of user account information that was compromised makes this possibly the single largest data breach in history.

But what would they even want with your personal email account? Plenty. The hackers made off with names, user names, hashed passwords, telephone numbers, and even birthdates and security questions. While no Social Security numbers should have been involved in the stored data, what was accessed is enough to do a world of identity theft damage.

2016 Data Breaches

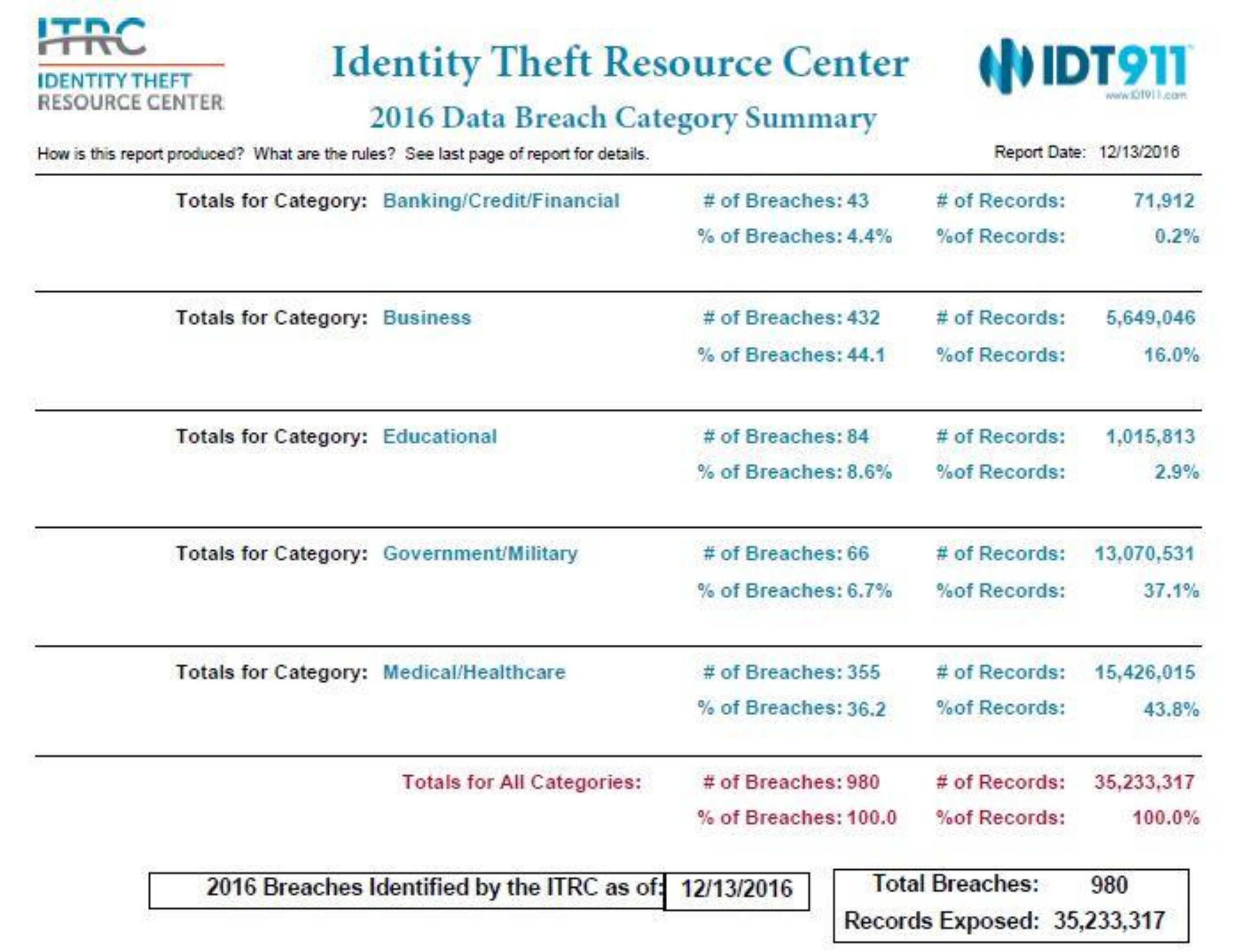
(First 6 months)

First Six Months of 2016 Data Breach Trends

- There were 1,837 incidents reported during the first six months of 2016 exposing over 1.1 billion records.
- Top 10 breaches (8 Hacks and 2 Web), exposed a combined 962.2 million records.
- Top 10 Severity scores averaged 9.69 out of 10.0.
- The Business sector accounted for 51.6% of reported incidents, followed by Unknown (22.6%), Medical (10.7%), Government (10.5%), and Education (4.6%).
- The Business sector accounted for 65.5% of the number of records exposed, followed by Unknown (19.6%), Government (14.6%), Medical (.3%), and Education < .1%.
- 50.8% of reported incidents were the result of Hacking, which accounted for 83.4% of the exposed records.
- Web accounted for 14.5% of the exposed records, but represented just 3.3% of the reported incidents.
- Breaches involving U.S. entities accounted for 52.3% of the incidents and 68.1% of the exposed records.
- 40.5% of the incidents exposed at between one and 1000 records.
- 131 incidents involved Third Parties
- Thirty--three (33) incidents so far in 2016 exposed more than one million records.
- Two 2016 incidents have taken their place on the Top 10 List All Time at Number One and Number Five.
- Five incidents have involved Voter Records exposing more 368 million persons.
- The number of reported incidents tracked by Risk Based Security has exceeded 21,000 exposing over 5.8 billion records.

https://www.riskbasedsecurity.com/2016/08/data-breaches-lead-to-over-1-billion-records-exposed-in-the-first-half-of-2016/

Data Breaches 2016



Identity Theft Resource Center

2016 Data Breach Category Summary

How is this report produced? What are the rules? See last page of report for details.

Report Date: 12/13/2016

Totals for Category:	Banking/Credit/Financial	# of Breaches: 43	# of Records:	71,912
		% of Breaches: 4.4%	%of Records:	0.2%
Totals for Category:	Business	# of Breaches: 432	# of Records:	5,649,046
		% of Breaches: 44.1	%of Records:	16.0%
Totals for Category:	Educational	# of Breaches: 84	# of Records:	1,015,813
		% of Breaches: 8.6%	%of Records:	2.9%
Totals for Category:	Government/Military	# of Breaches: 66	# of Records:	13,070,531
		% of Breaches: 6.7%	%of Records:	37.1%
Totals for Category:	Medical/Healthcare	# of Breaches: 355	# of Records:	15,426,015
		% of Breaches: 36.2	%of Records:	43.8%
Totals for All Categories:		# of Breaches: 980	# of Records:	35,233,317
		% of Breaches: 100.0	%of Records:	100.0%

2016 Breaches Identified by the ITRC as of: 12/13/2016

Total Breaches: 980
Records Exposed: 35,233,317

http://www.idtheftcenter.org/

Data Breaches 2016

itrc Identity Theft Resource Center

2015 Data Breach Stats

IDT911 www.IDT911.com

2016 Breaches Identified by the ITRC as of: 12/13/2016

Total Breaches: 980
Records Exposed: 35,233,317

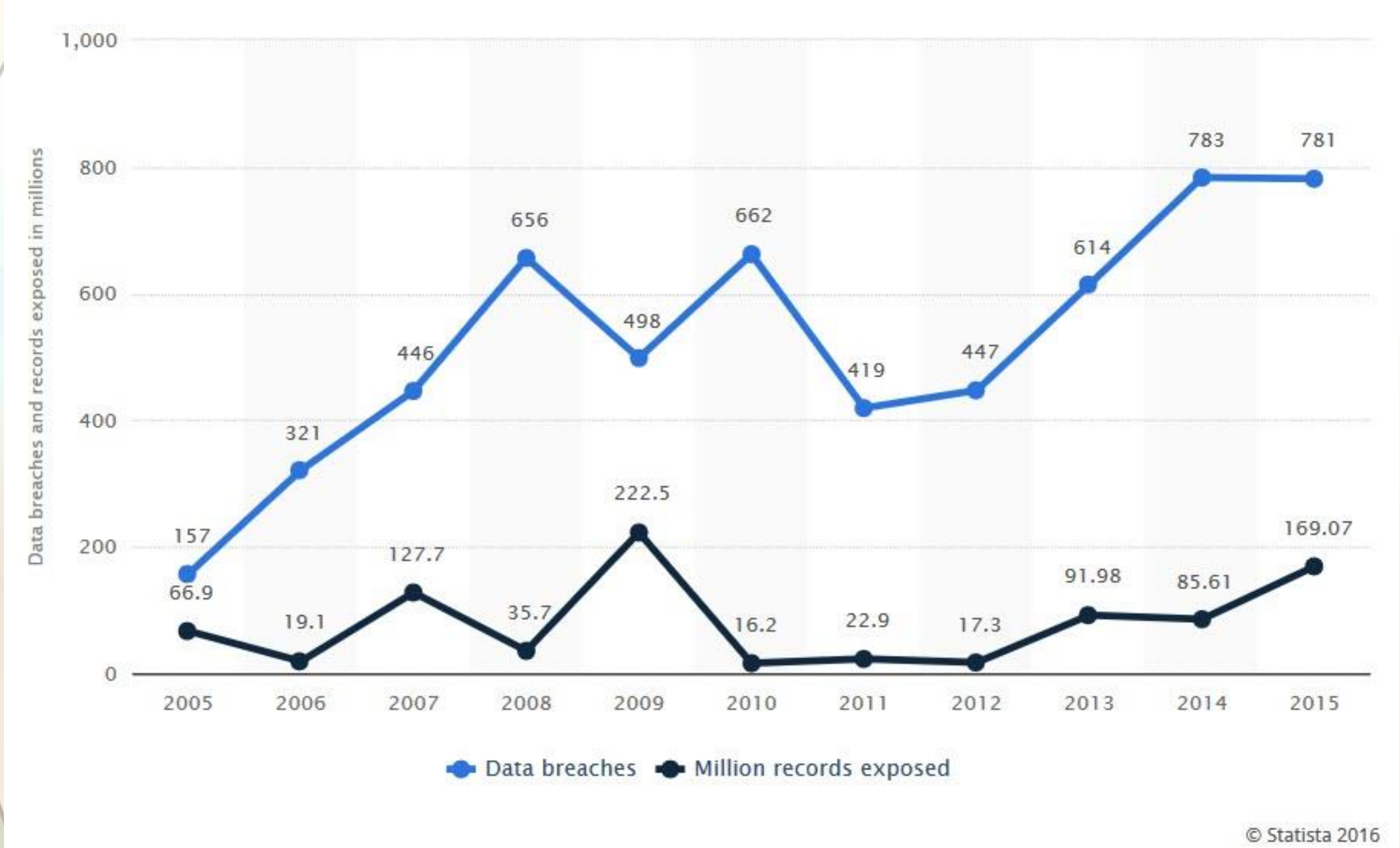
http://www.idtheftcenter.org/

Data Breaches 2005 – Dec 13, 2016

Number of breaches = 6,789

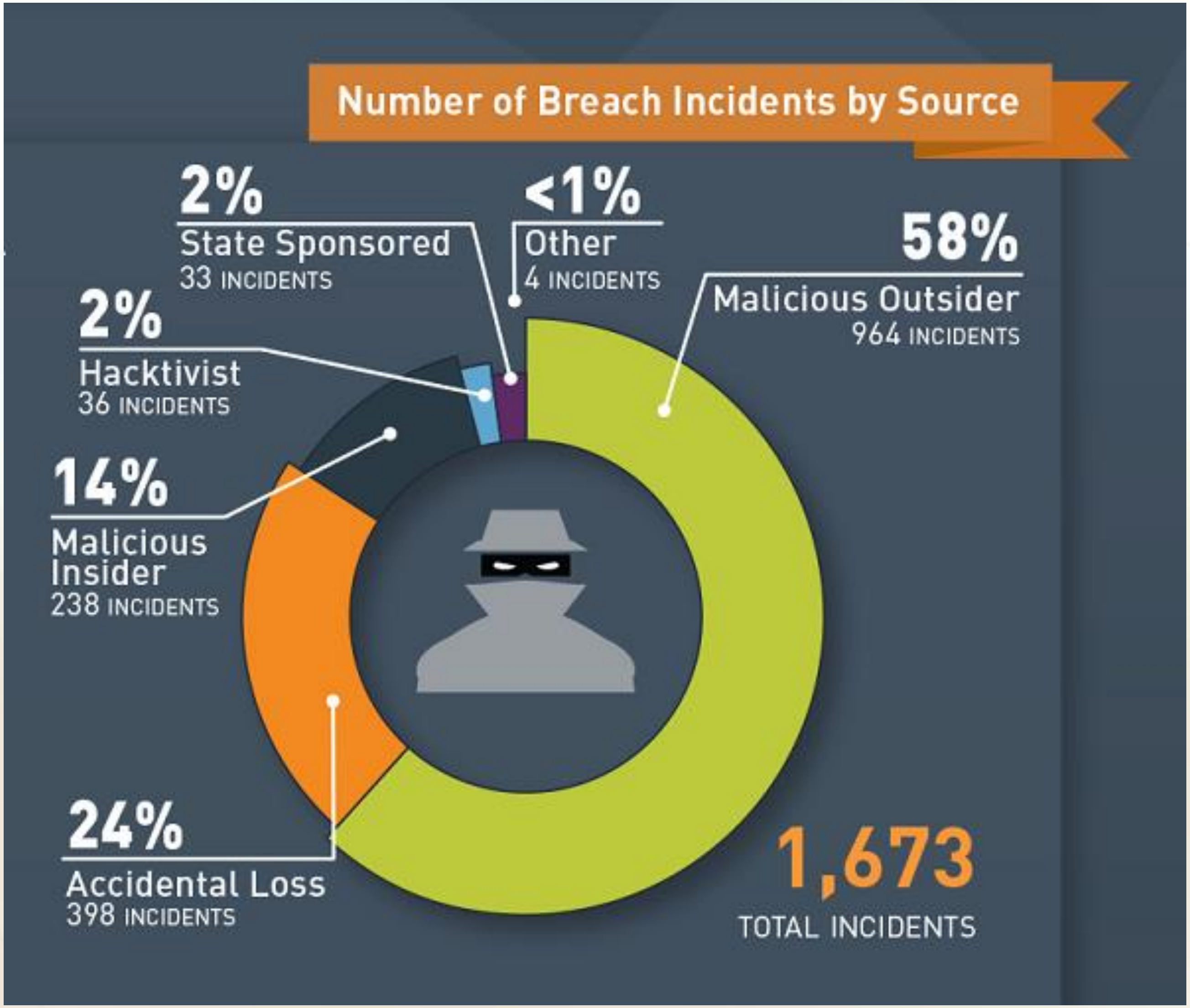
Number of Records = 886,544,750

http://www.idtheftcenter.org/Data-Breaches/data-breaches.html



https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Breach Sources 2015



http://blog.gemalto.com/security/2016/03/03/2015-data-breaches-by-the-numbers/

You Weren't Hacked, You Were Spoofed

Has someone requested you to be Facebook friends, when you already are? They weren't hacked, they were Spoofed. Has one of your friends on Facebook told you that they received a request from you to be friends? You Weren't Hacked, You Were Spoofed !

Hacked: someone has used a computer to gain unauthorized access to your computer.
Spoofed: someone has set up a fake profile pretending to be you in order to gain access to your friends and their personal information shared on Facebook.

The difference is important to understand. If someone is pretending to be you by using a spoofed profile they don't have access to any information that you don't already have available to the public. They are hoping that your friends will accept the new spoofed friend request so that they will have access to whatever information your friends have made available to the public, but more important what they made available to Facebook friends only. It isn't you that is at risk, it is your friends who accept the spoofed friend request. If you get a friend request and you know it is a spoofer, please report it ASAP. The quicker it is reported; the safer people will be.

Use this address to get instructions on what to do to report spoofing.
https://www.dropbox.com/s/dd97q9mh0wpw6y6/You%20Werent%20Hacked,%20You%20Were%20Spoofed%20on%20Facebook.pdf?dl=0

ATM Scam

Bank ATMs converted to steal bank customer IDs

A team of organized criminals installs equipment on legitimate bank ATMs to steal both the ATM card number and the PIN.

TBO.com Source editor The Tampa Tribune
Published: August 15, 2014

Hillsborough County sheriff's deputies are searching for a person seen in surveillance images attaching a skimming device to an ATM at a Tampa bank.

About 6:30 p.m. Wednesday, the person used green tape and a clear, gluelike substance to attach the card reader to an ATM at Regions Bank, 6297 W. Waters Ave., deputies said.

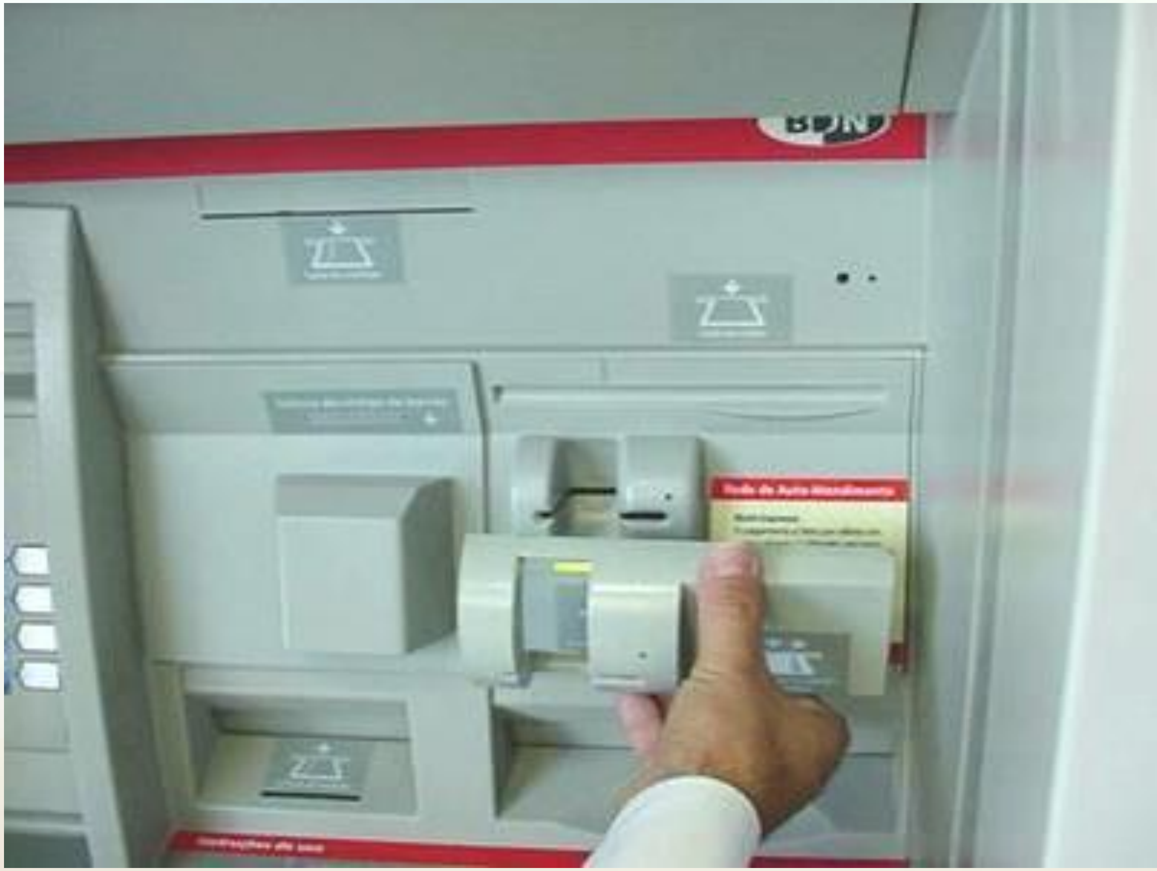
The small, thin, square silver device was affixed to the front underside of the ATM, above the keypad area, deputies said. Investigators said the box contained electronics and a camera to record customers' fingers as they entered PIN numbers on the keypad

* Posted on Feb 4, 2015 by Bret Kanapaux WWSB-TV mysuncoast.com Sarasota, FL

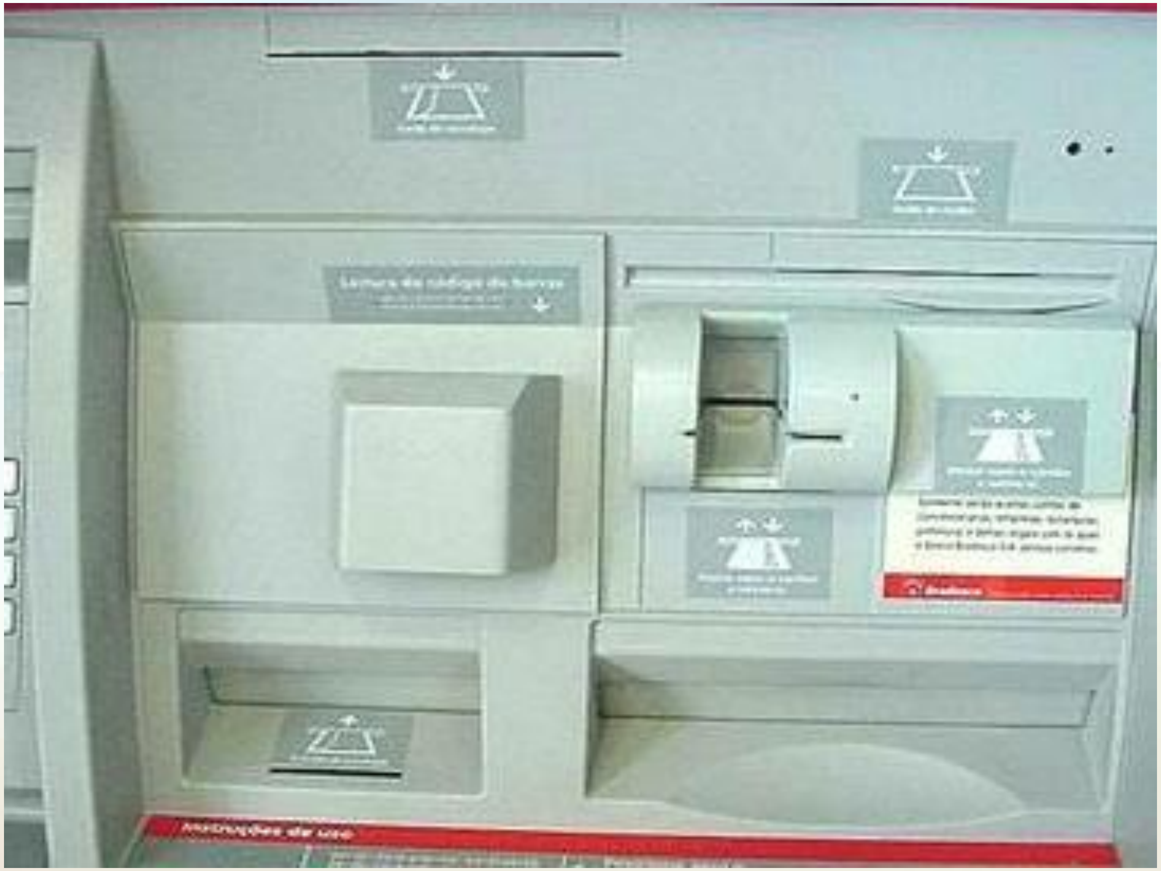
SARASOTA, Fla. -- Anyone who used the ATM at the Sun Trust Bank near the Westfield Southgate Mall should check their bank account. Police say a card skimmer was placed at that location in the past week, and investigators believe it's the work of the same suspect who placed a skimmer at the Sun Trust ATM on Main Street.

A victim contacted Sarasota Police detectives, who discovered that at 10:20 a.m. on Sat., Jan. 31, the suspect installed the skimmer at the Sun Trust Bank branch at 3400 South Tamiami Trail. The suspect returned a few hours later at 1:40 p.m. and removed the device.

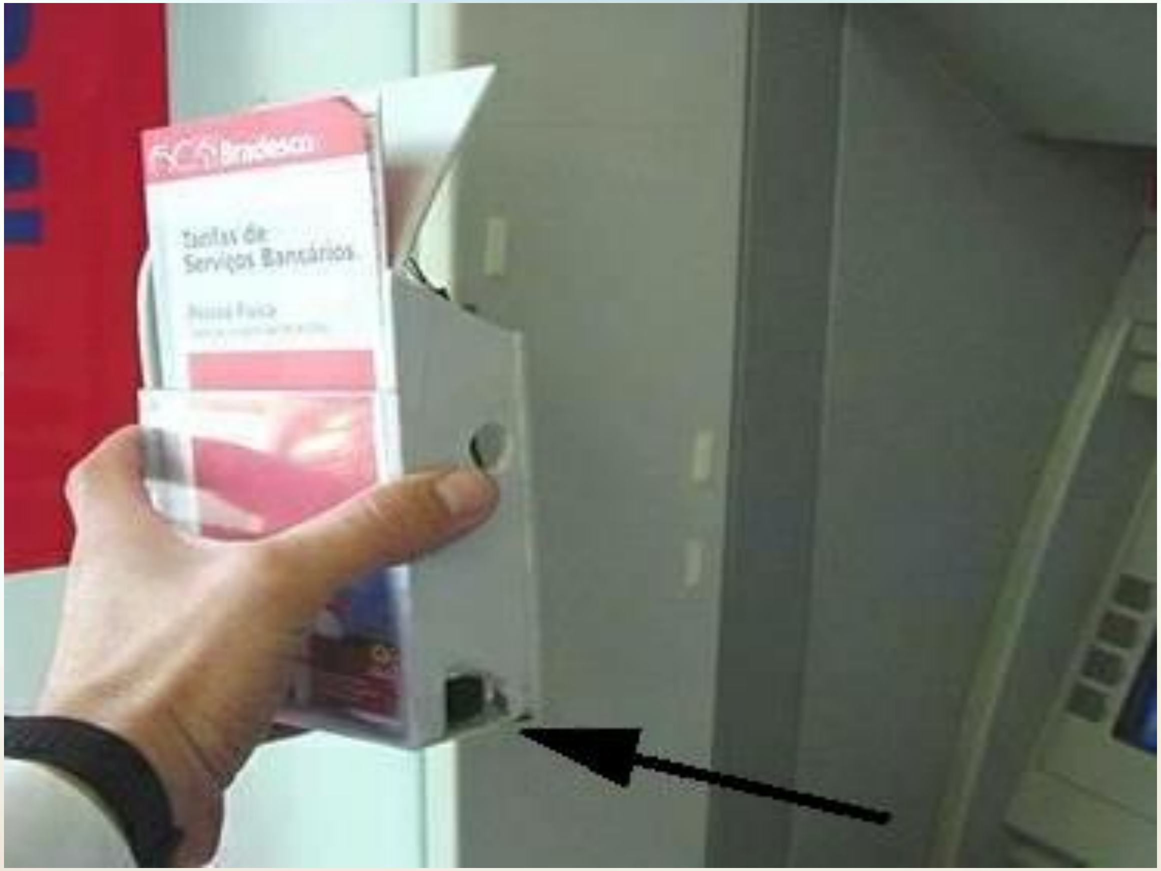
2_min_23_sec_v_skimmers_hernando_WFTS-TV



Equipment being installed on front of existing bank card slot.



The equipment as it appears installed over the normal ATM bank slot.



The PIN reading camera being installed on the ATM is housed in an innocent looking leaflet enclosure.

The camera shown installed and ready to capture PINs by looking down on the keypad as you enter your PIN.

Precaution at the ATM Machine

- Cover your PIN Number
- Don’t Leave the ATM Machine Too Early
- Shake, Rattle and Roll
- Use ATM Machines Inside of Banks
- Monitor Your Account Activity

Group stole card numbers with 'skimmers'

From the Orlando Sentinel November 2, 2011

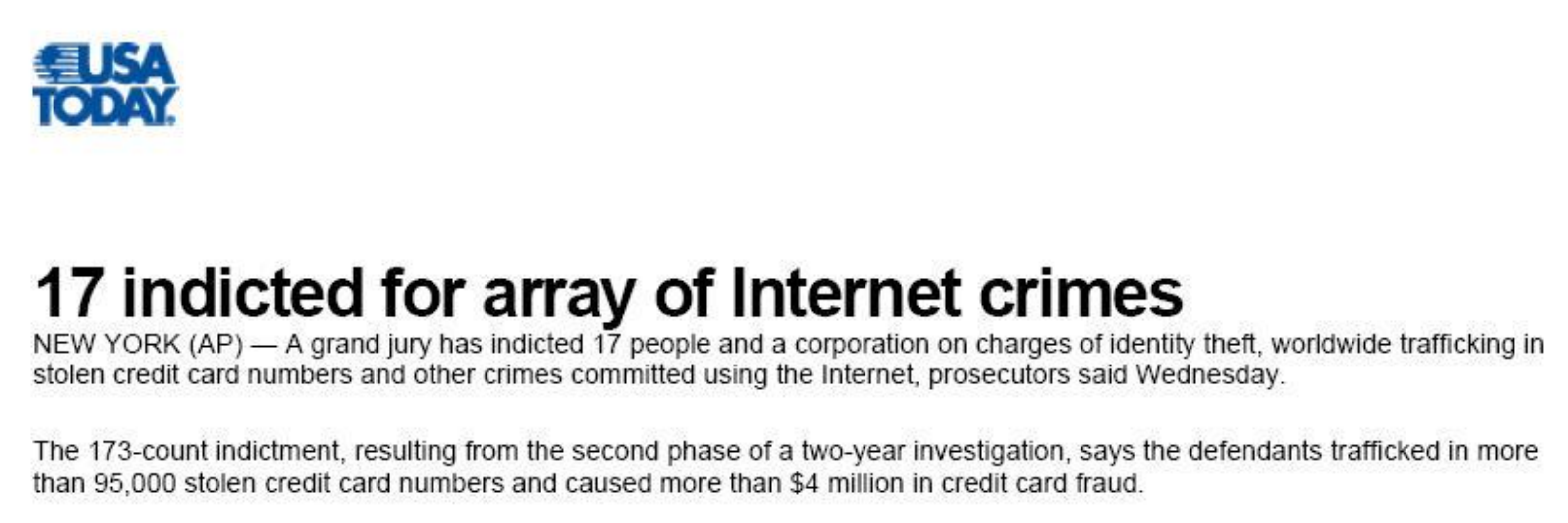
Federal authorities have accused owners of an Orlando mobile-phone business of using stolen credit-card numbers — obtained via "skimming" devices implanted at gas stations — to buy hundreds of thousands of dollars of merchandise at area stores.

Agents say the group obtained credit-card numbers from skimming devices that were installed on Central Florida gas-station pumps, and then used equipment to manufacture credit cards, debit cards and gift cards with the stolen numbers.

American Express identified about **$125,565** worth of fraudulent charges at Target related to the case, and Discover identified about **$30,220**, court documents said.

American Express said the credit-card numbers were stolen at a **Hess gas station in Winter Springs.** The Secret Service accuses the group of using more than 175 fraudulent credit cards between January and October.

The Bad Guys Do Get Caught



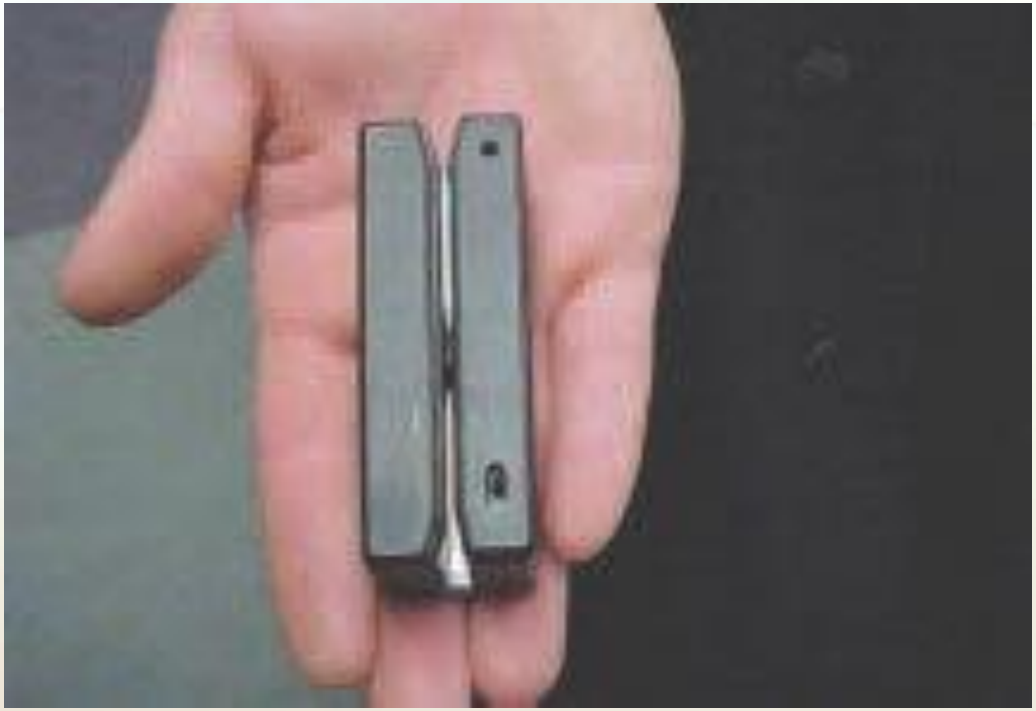
USA TODAY

17 indicted for array of Internet crimes

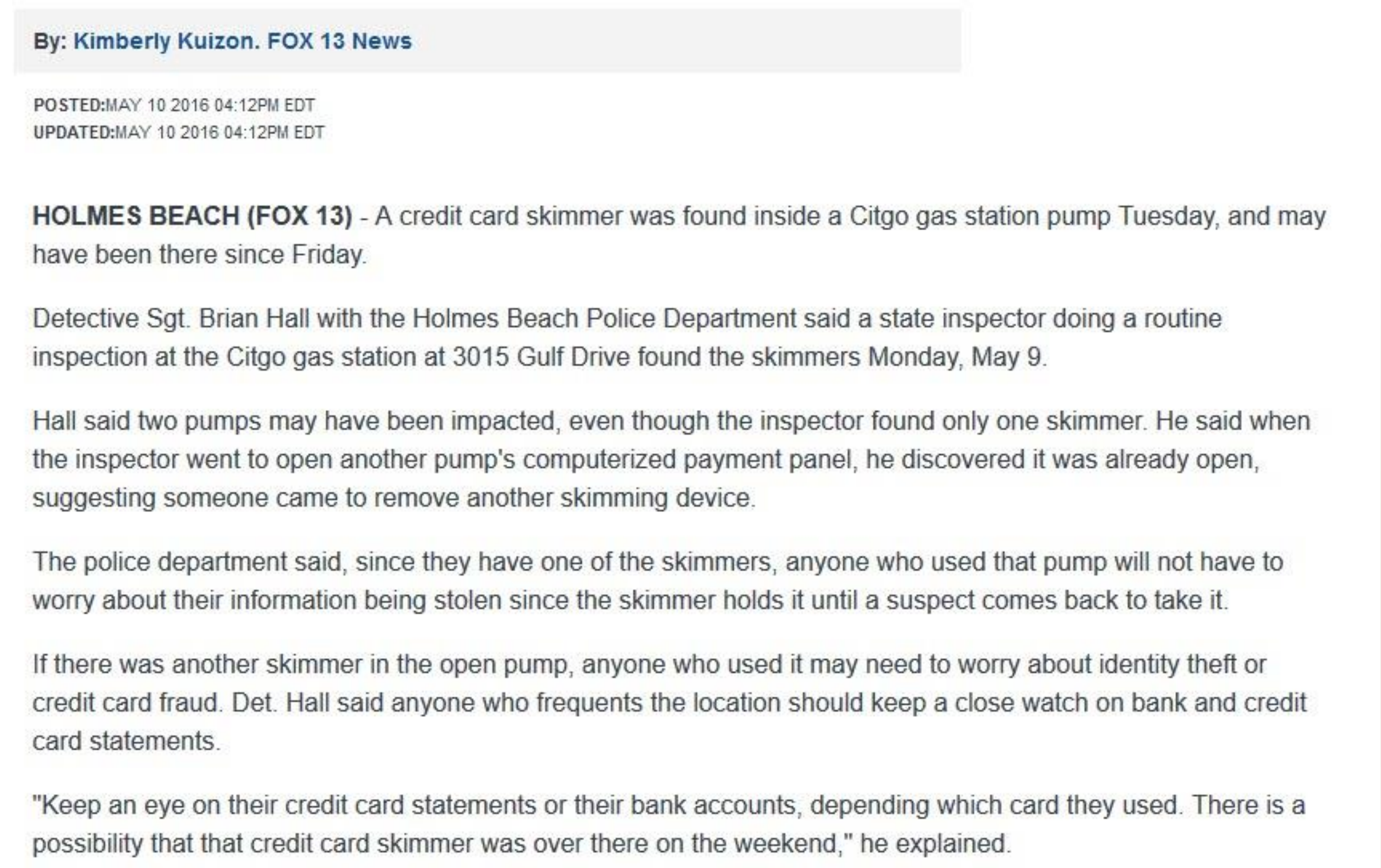
NEW YORK (AP) — A grand jury has indicted 17 people and a corporation on charges of identity theft, worldwide trafficking in stolen credit card numbers and other crimes committed using the Internet, prosecutors said Wednesday.

The 173-count indictment, resulting from the second phase of a two-year investigation, says the defendants trafficked in more than 95,000 stolen credit card numbers and caused more than $4 million in credit card fraud.

A Hand Skimmer



Skimmer in Gas Pump



By: Kimberly Kuizon. FOX 13 News

POSTED:MAY 10 2016 04:12PM EDT
UPDATED:MAY 10 2016 04:12PM EDT

HOLMES BEACH (FOX 13) - A credit card skimmer was found inside a Citgo gas station pump Tuesday, and may have been there since Friday.

Detective Sgt. Brian Hall with the Holmes Beach Police Department said a state inspector doing a routine inspection at the Citgo gas station at 3015 Gulf Drive found the skimmers Monday, May 9.

Hall said two pumps may have been impacted, even though the inspector found only one skimmer. He said when the inspector went to open another pump's computerized payment panel, he discovered it was already open, suggesting someone came to remove another skimming device.

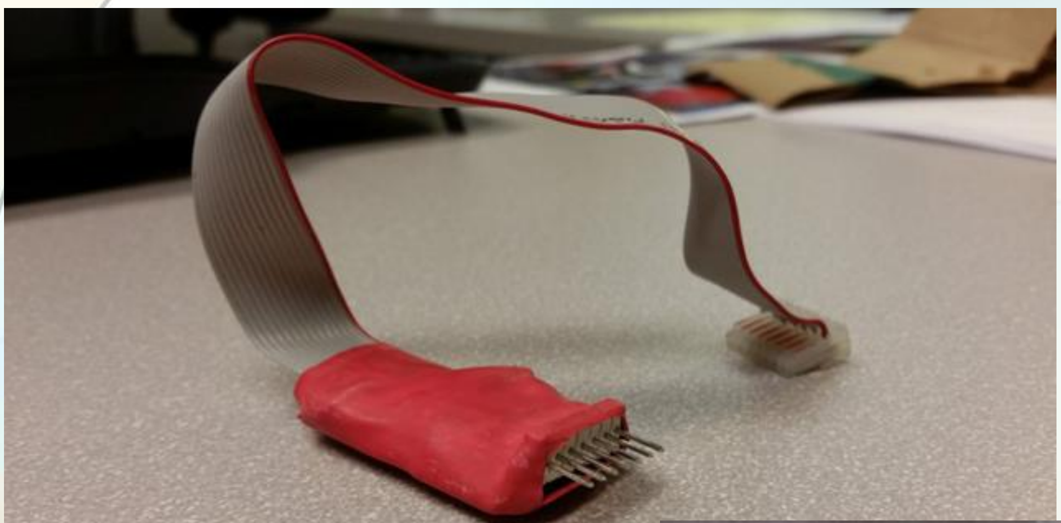
The police department said, since they have one of the skimmers, anyone who used that pump will not have to worry about their information being stolen since the skimmer holds it until a suspect comes back to take it.

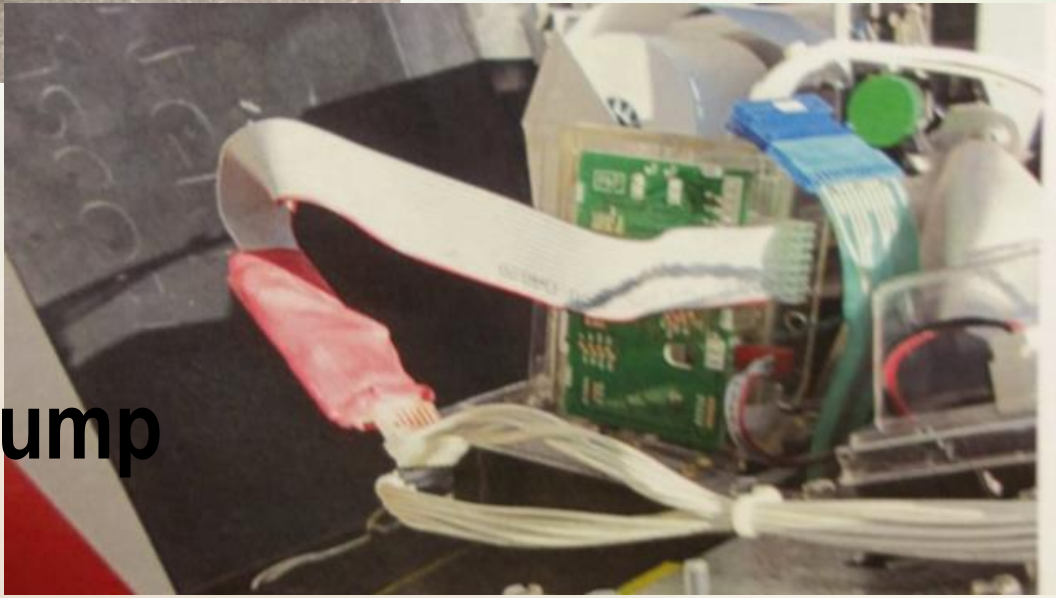
If there was another skimmer in the open pump, anyone who used it may need to worry about identity theft or credit card fraud. Det. Hall said anyone who frequents the location should keep a close watch on bank and credit card statements.

"Keep an eye on their credit card statements or their bank accounts, depending which card they used. There is a possibility that that credit card skimmer was over there on the weekend," he explained.

http://www.fox13news.com/news/local-ews/139585233-story

The Skimmer





Inside the pump

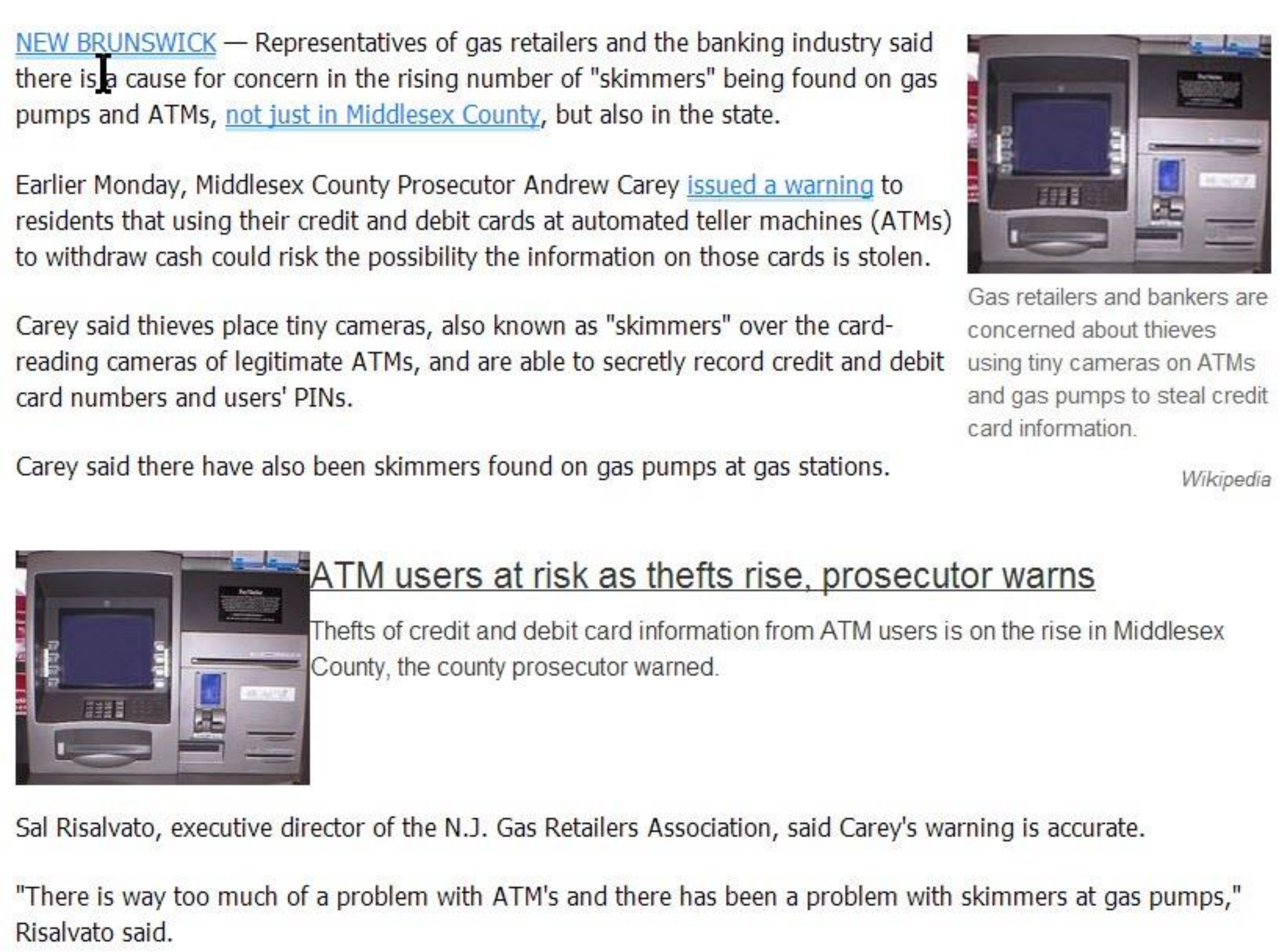
Pump Safety Tips

When you buy gas, you should remember these safety tips:

1. Pay with cash inside the store when possible. If you don’t have cash, use a credit card instead of a debit card. Credit cards have better fraud protection.
2. Check for signs of tampering at the pump. This includes a broken security seal over the door. If something seems out of place, notify gas station personnel.
3. Monitor bank statements regularly to spot unauthorized charges. If something doesn’t add up, contact your bank immediately.

http://wfla.com/2016/03/07/credit-card-skimmers-discovered-at-sarasota-gas-station/

NJ: Skimmers – A Growing Problem



NEW BRUNSWICK — Representatives of gas retailers and the banking industry said there is a cause for concern in the rising number of "skimmers" being found on gas pumps and ATMs, not just in Middlesex County, but also in the state.

Earlier Monday, Middlesex County Prosecutor Andrew Carey issued a warning to residents that using their credit and debit cards at automated teller machines (ATMs) to withdraw cash could risk the possibility the information on those cards is stolen.

Carey said thieves place tiny cameras, also known as "skimmers" over the card-reading cameras of legitimate ATMs, and are able to secretly record credit and debit card numbers and users' PINs.

Carey said there have also been skimmers found on gas pumps at gas stations.

Gas retailers and bankers are concerned about thieves using tiny cameras on ATMs and gas pumps to steal credit card information.

Wikipedia

ATM users at risk as thefts rise, prosecutor warns

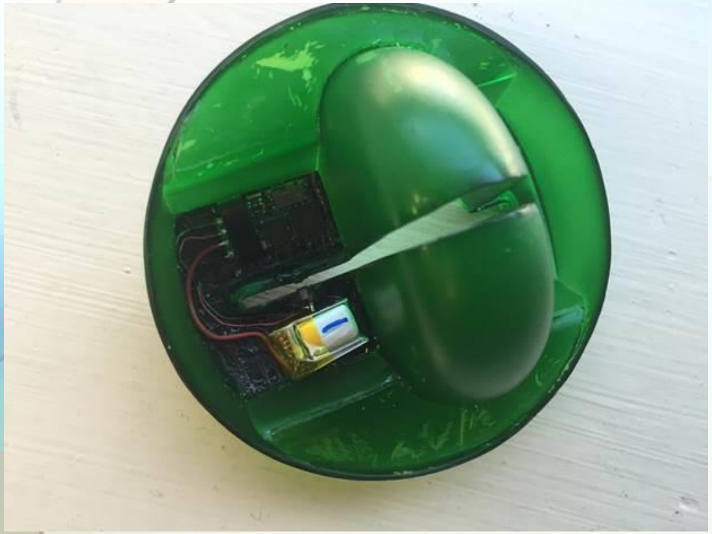
Thefts of credit and debit card information from ATM users is on the rise in Middlesex County, the county prosecutor warned.

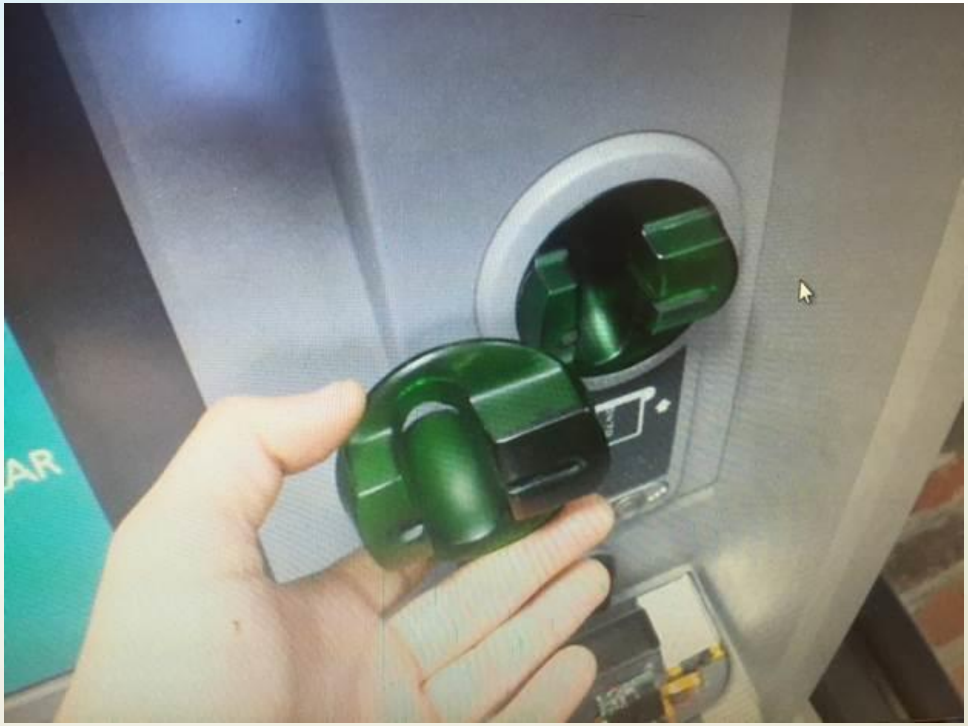
Sal Risalvato, executive director of the N.J. Gas Retailers Association, said Carey's warning is accurate.

"There is way too much of a problem with ATM's and there has been a problem with skimmers at gas pumps," Risalvato said.

http://www.nj.com/middlesex/index.ssf/2016/02/gas_retailers_bankers_voice_concerns_about_atm_ski.html

Bank Skimmers





Security Freeze

A security freeze is a notice that is placed in a consumer's credit report (on request of the consumer) that prohibits a credit reporting agency (such as **Equifax**, **Experian** or **TransUnion**) from releasing the consumer's credit report, credit score or any information contained within the consumer report to a third party without the express authorization of the consumer.

However, the credit reporting agency can notify the third party that a security freeze has been placed on the consumer's credit files.

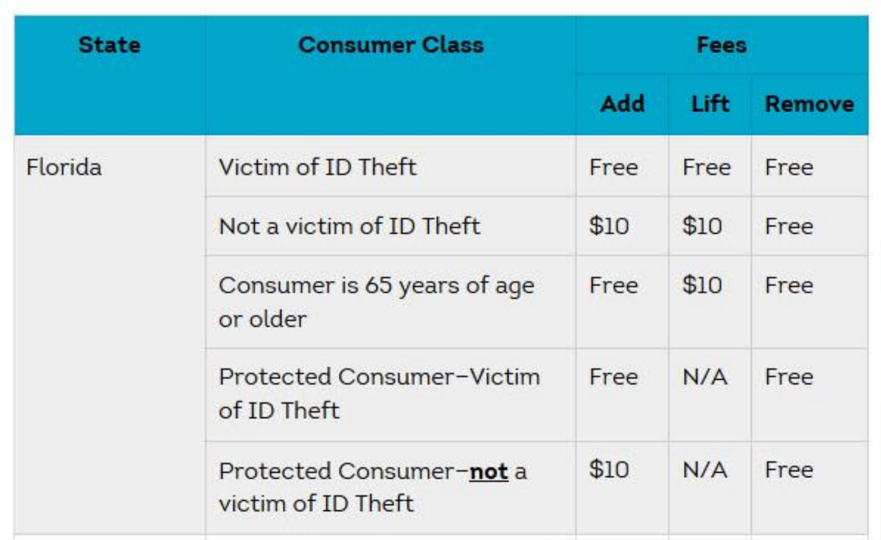
http://www.freshfromflorida.com/Consumer-Resources/Consumer-Protection/Scams-and-Fraud/Identity-Theft/Security-Freeze-Credit-Report-FAQ

Security Freeze

When should I consider a security freeze?

- You want maximum control over access to your credit report.
- You are concerned that you might become a victim of fraud/ID theft.
- You are a victim of fraud/ID theft.
- You won’t need to apply for credit in the foreseeable future.
- You are the guardian of a minor or medically incapacitated consumer who won’t need to apply for credit in the foreseeable future.

Florida Freeze Fees



State	Consumer Class	Fees		
		Add	Lift	Remove
Florida	Victim of ID Theft	Free	Free	Free
	Not a victim of ID Theft	$10	$10	Free
	Consumer is 65 years of age or older	Free	$10	Free
	Protected Consumer–Victim of ID Theft	Free	N/A	Free
	Protected Consumer–**not** a victim of ID Theft	$10	N/A	Free

- 1. Seniors over 65 can freeze all three CRB for free, as well as those who have had identity theft
- 2. Seniors over 65 can permanently unfreeze the accounts for free
- 3. Seniors over 65 have to pay the $10 to temporarily unfreeze and pay $10 to re-freeze any or each CRB for any reason
- 4. The fee does not apply to victims of identity theft

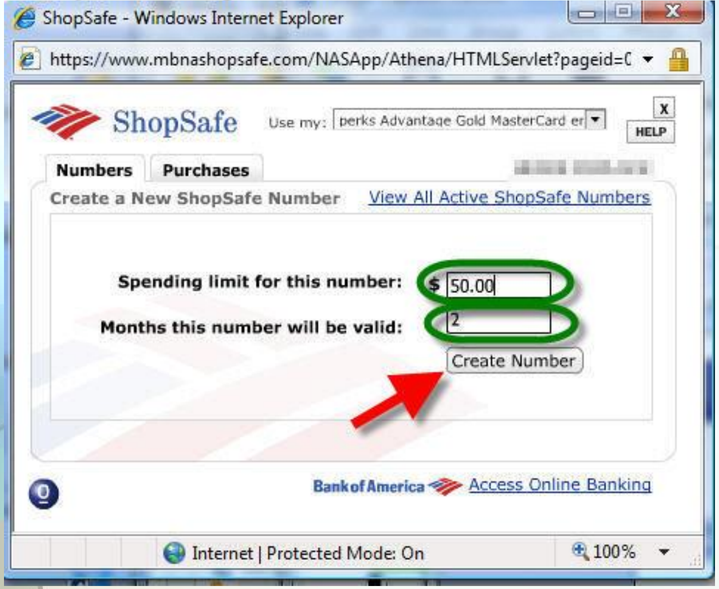
http://www.transunion.com/credit-freeze/place-credit-freeze

http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx

Safe Shopping Tips

- **Shop Where You're Safe:** Wi-Fi is great, but when you're shopping online it pays to use a secure connection.
- **Look for the Padlock:** Not sure you're logged onto a safe URL? Secure websites start with "https" rather than "http". In addition, your Web browser will always display a key or closed padlock icon
- **Don't Shop at Random Stores:** If the website you're dealing with still makes you raise an eyebrow, look them up on the Better Business Bureau's website
- **Do Not Use Debit Cards:** The Privacy Rights Clearinghouse recommends that consumers never use (or even carry) debit cards (also known as check cards) because of their risks and their limited consumer protections.
- **Use a Virtual Credit Card:** Virtual credit card numbers are linked to your credit card, but unlike your credit card, virtual numbers are only good for one transaction or limited to a predetermined dollar amount. They're available from most banks like Citi, Bank of America, and Discover, providing an extra layer of protection when shopping online

ShopSafe


ShopSafe - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=C
ShopSafe
HELP
Numbers
Purchases
View All Active ShopSafe Numbers
Create Number
Bank of America
Access Online Banking
Internet | Protected Mode: On
100%

Use my: perks Advantage Gold MasterCard er

[redacted]

Create a New ShopSafe Number

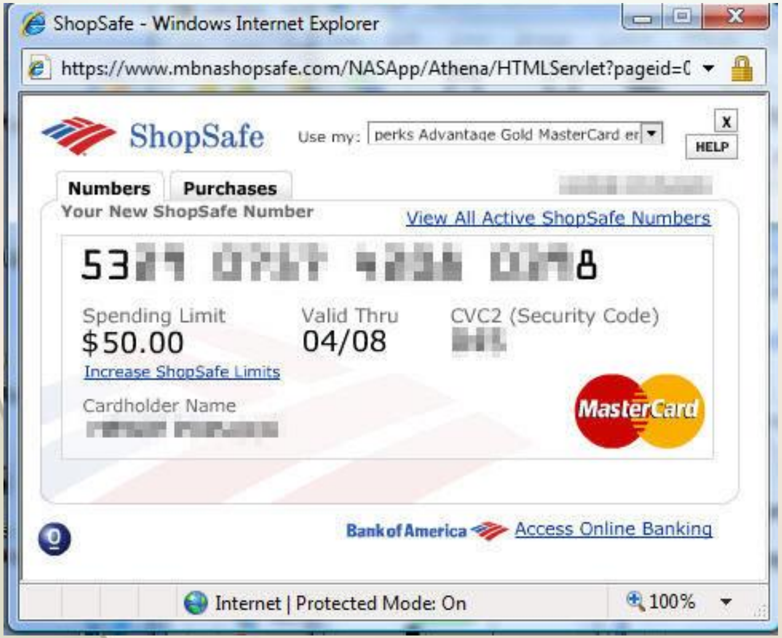
Spending limit for this number: $ 50.00

Months this number will be valid: 2

How it works

Shop online as usual. When it’s time to make your purchase, just log in to ShopSafe. You'll need the 3-digit security code located on the back of your physical credit card.

Enter your spending limits, and ShopSafe will automatically generate a temporary account number with expiration date and security code that allows you to complete your purchase while protecting your privacy. Each ShopSafe number can only be used at one merchant.


ShopSafe - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=C
ShopSafe
HELP
Numbers
Purchases
View All Active ShopSafe Numbers
Increase ShopSafe Limits
MasterCard
Bank of America
Access Online Banking
Internet | Protected Mode: On
100%

Use my: perks Advantage Gold MasterCard er

[redacted]

Your New ShopSafe Number

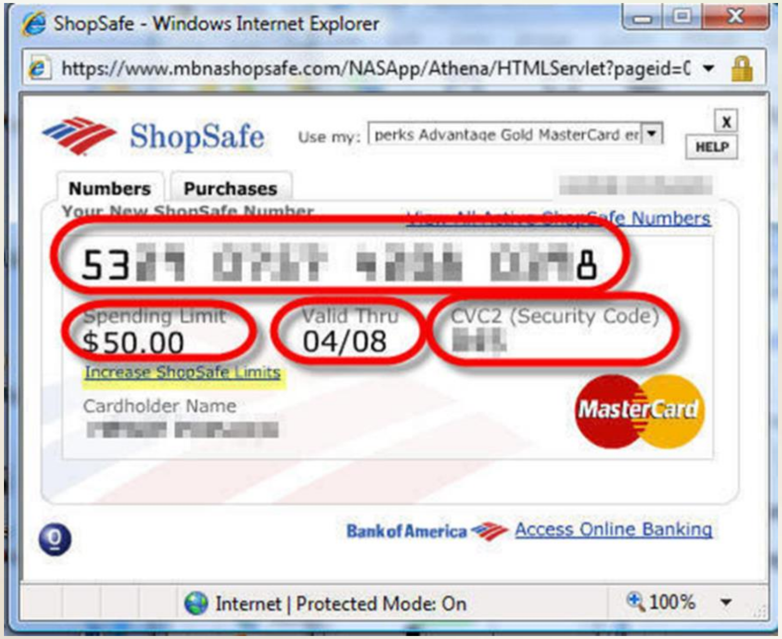
53[redacted]8

Spending Limit $50.00

Valid Thru 04/08

CVC2 (Security Code) [redacted]

Cardholder Name [redacted]


ShopSafe - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=C
ShopSafe
HELP
Numbers
Purchases
View All Active ShopSafe Numbers
Increase ShopSafe Limits
MasterCard
Bank of America
Access Online Banking
Internet | Protected Mode: On
100%

Use my: perks Advantage Gold MasterCard er

[redacted]

Your New ShopSafe Number

53[redacted]8

Spending Limit $50.00

Valid Thru 04/08

CVC2 (Security Code) [redacted]

Cardholder Name [redacted]

Blur Uses One-Time Use Credit Card Numbers to Deter Hackers

- After all the recent credit hacking news, many people are a little more hesitant about using plastic. Blur is a service that makes your shopping a little more secure by generating "fake" credit card numbers to deter hackers.

- Blur is a browser extension and mobile app. One of its most appealing features is credit card masking, which allows you to buy items without actually giving out any information. The feature a premium level which costs $39.00 a year ($3 a month).

https://dnt.abine.com

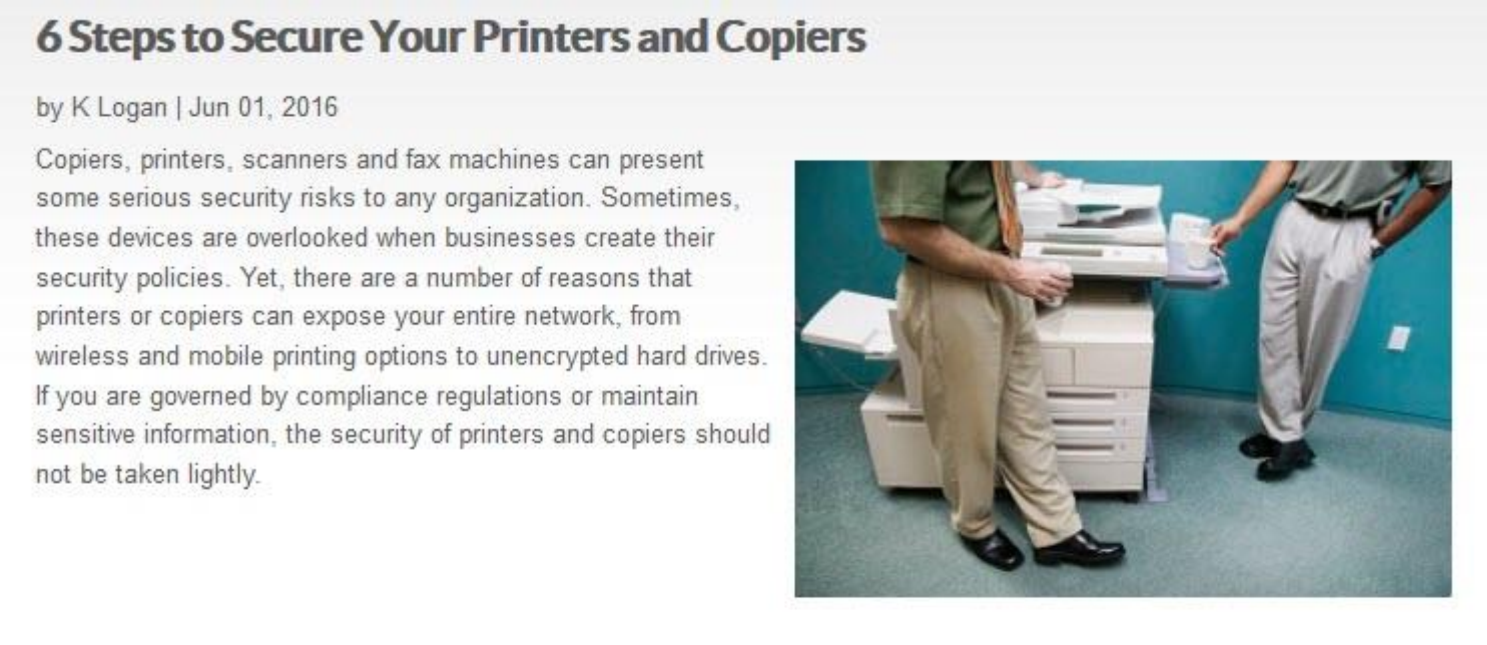
New Chips in Credit Cards

*The chips in our credit cards are EMV chips. **EMV** stands for Europay, Mastercard, and Visa. These chips are not the true **RFID** chips we spent all that time dreading. Some chipped cards are capable of near-field communications (NFC) — which are indeed radio-frequency communications, but effective only at extremely short distances.*

Credit Card Chips

2min_43sec_v_CreditCard Chips

Printers & Copiers



6 Steps to Secure Your Printers and Copiers

by K Logan | Jun 01, 2016

Copiers, printers, scanners and fax machines can present some serious security risks to any organization. Sometimes, these devices are overlooked when businesses create their security policies. Yet, there are a number of reasons that printers or copiers can expose your entire network, from wireless and mobile printing options to unencrypted hard drives. If you are governed by compliance regulations or maintain sensitive information, the security of printers and copiers should not be taken lightly.

- Most commercial digital copiers use disk drives to reproduce documents.

- The same machines that are commonly used to spit out copies of tax returns for millions of Americans can retain the data being scanned.

- If the data on the copier's disk aren't protected with encryption or an overwrite mechanism, and if someone with malicious motives gets access to the machine, industry experts say sensitive information from original documents could get into the wrong hands.

Theft after Death

What Is Ghosting Identity Theft?

Identity thieves can strike anyone, including children and senior citizens — and increasingly, they're also targeting people who've passed away.

Called "ghosting," this type of identity theft involves about 2.5 million deceased individuals each year, according to the IRS. Criminals use information like Social Security number, previous addresses, birthdate and employment history to apply for loans, obtain medical services and open credit card accounts.

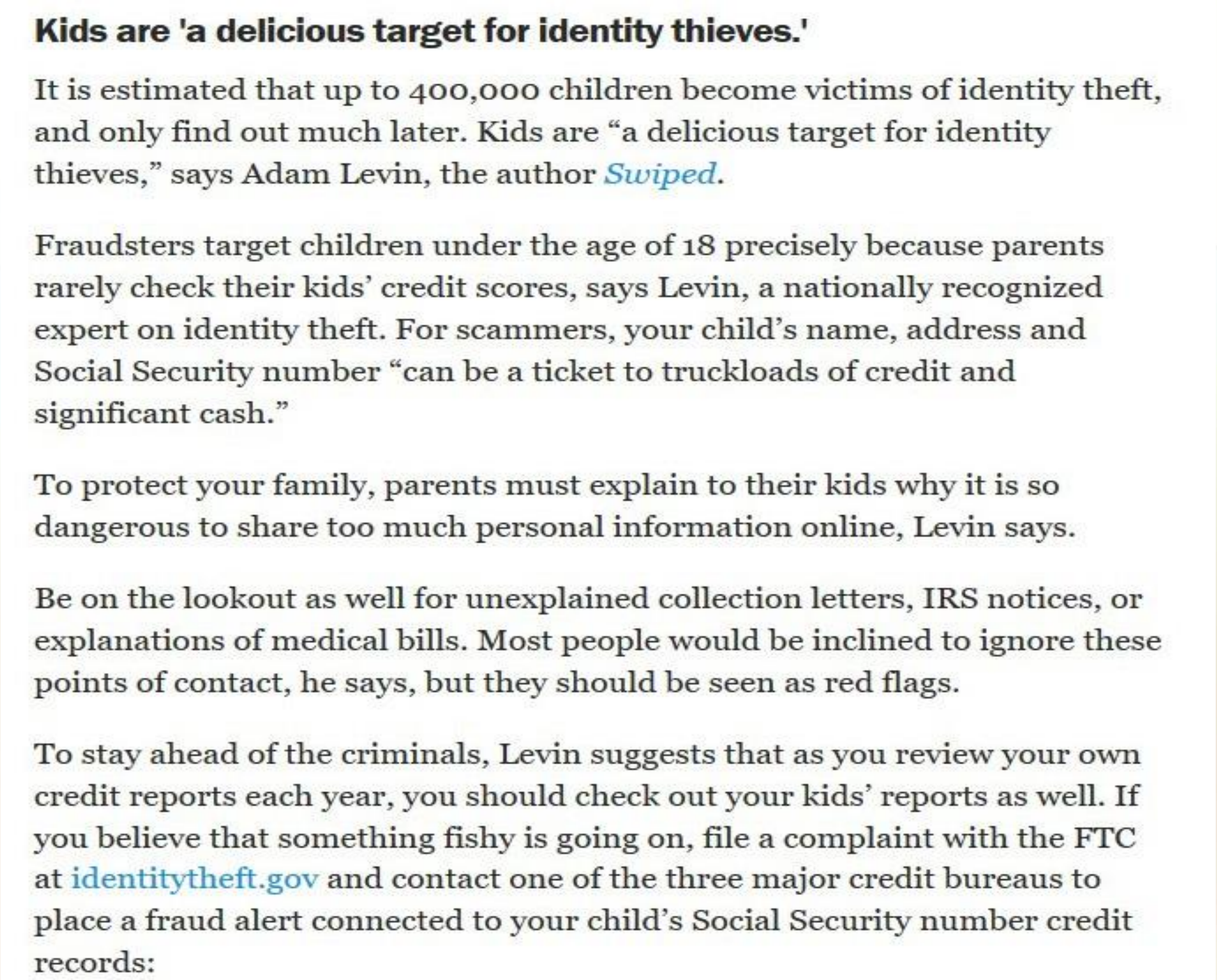
During the early part of every year, there's a sharp uptick in fraudulent tax returns that are filed with the identities of deceased persons. The IRS estimates that annual refunds related to ghosting identity theft total about $5 billion.

Children & ID Theft

Protect your children

The latest tactic these crooks are using is to steal the identity of children, preferably infants! Order a credit report on each of your minor children at least once each year.

Children & ID Theft



Kids are 'a delicious target for identity thieves.'

It is estimated that up to 400,000 children become victims of identity theft, and only find out much later. Kids are "a delicious target for identity thieves," says Adam Levin, the author *Swiped*.

Fraudsters target children under the age of 18 precisely because parents rarely check their kids' credit scores, says Levin, a nationally recognized expert on identity theft. For scammers, your child's name, address and Social Security number "can be a ticket to truckloads of credit and significant cash."

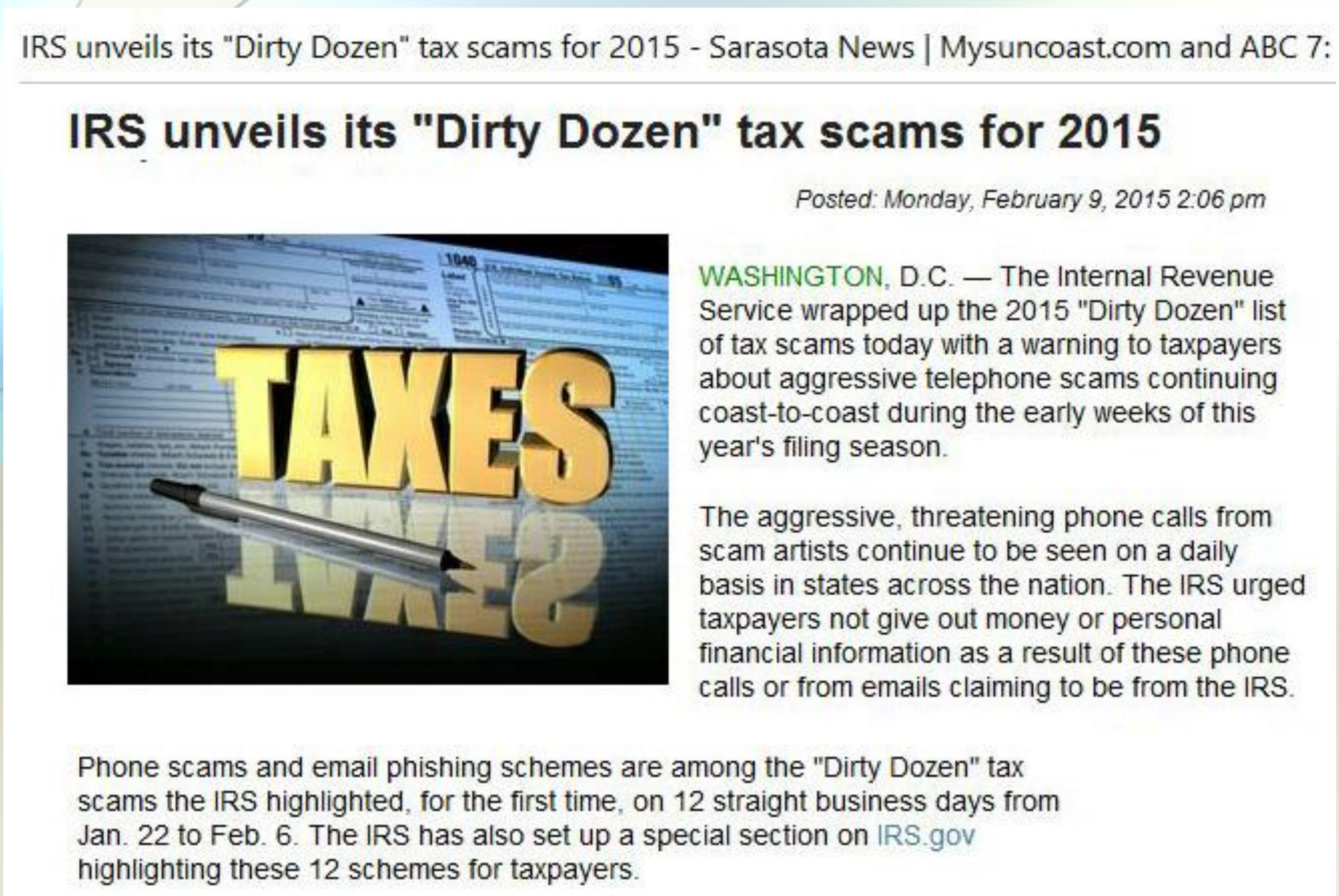
To protect your family, parents must explain to their kids why it is so dangerous to share too much personal information online, Levin says.

Be on the lookout as well for unexplained collection letters, IRS notices, or explanations of medical bills. Most people would be inclined to ignore these points of contact, he says, but they should be seen as red flags.

To stay ahead of the criminals, Levin suggests that as you review your own credit reports each year, you should check out your kids' reports as well. If you believe that something fishy is going on, file a complaint with the FTC at identitytheft.gov and contact one of the three major credit bureaus to place a fraud alert connected to your child's Social Security number credit records:

http://time.com/money/4367680/protect-kids-from-identity-theft/

IRS unveils its "Dirty Dozen" tax scams for 2015 - Sarasota News | Mysuncoast.com and ABC 7:



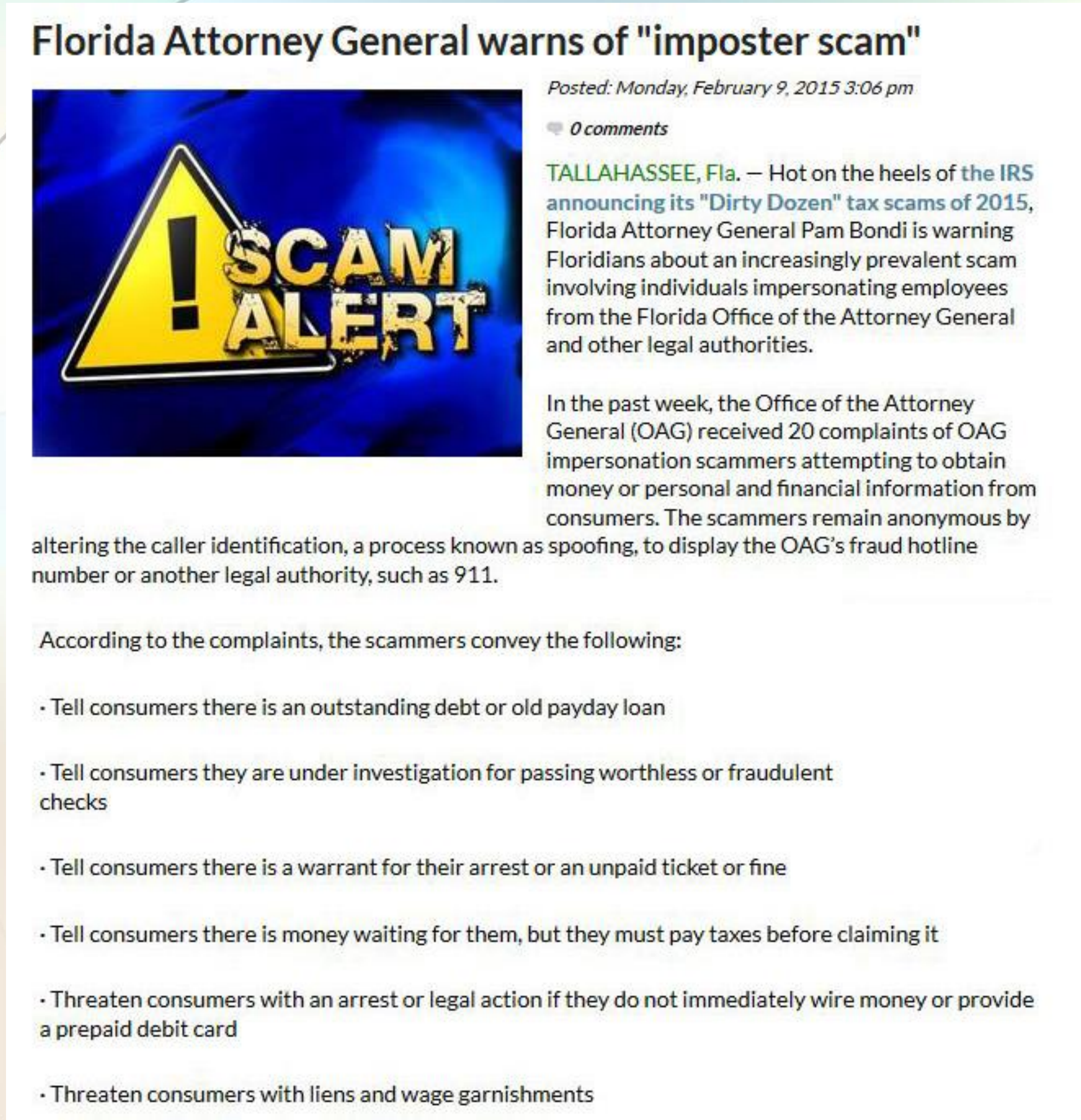
IRS unveils its "Dirty Dozen" tax scams for 2015

Posted: Monday, February 9, 2015 2:06 pm

WASHINGTON, D.C. — The Internal Revenue Service wrapped up the 2015 "Dirty Dozen" list of tax scams today with a warning to taxpayers about aggressive telephone scams continuing coast-to-coast during the early weeks of this year's filing season.

The aggressive, threatening phone calls from scam artists continue to be seen on a daily basis in states across the nation. The IRS urged taxpayers not give out money or personal financial information as a result of these phone calls or from emails claiming to be from the IRS.

Phone scams and email phishing schemes are among the "Dirty Dozen" tax scams the IRS highlighted, for the first time, on 12 straight business days from Jan. 22 to Feb. 6. The IRS has also set up a special section on IRS.gov highlighting these 12 schemes for taxpayers.



Florida Attorney General warns of "imposter scam"

Posted: Monday, February 9, 2015 3:06 pm

0 comments

TALLAHASSEE, Fla. — Hot on the heels of the IRS announcing its "Dirty Dozen" tax scams of 2015, Florida Attorney General Pam Bondi is warning Floridians about an increasingly prevalent scam involving individuals impersonating employees from the Florida Office of the Attorney General and other legal authorities.

In the past week, the Office of the Attorney General (OAG) received 20 complaints of OAG impersonation scammers attempting to obtain money or personal and financial information from consumers. The scammers remain anonymous by altering the caller identification, a process known as spoofing, to display the OAG's fraud hotline number or another legal authority, such as 911.

According to the complaints, the scammers convey the following:

· Tell consumers there is an outstanding debt or old payday loan

· Tell consumers they are under investigation for passing worthless or fraudulent checks

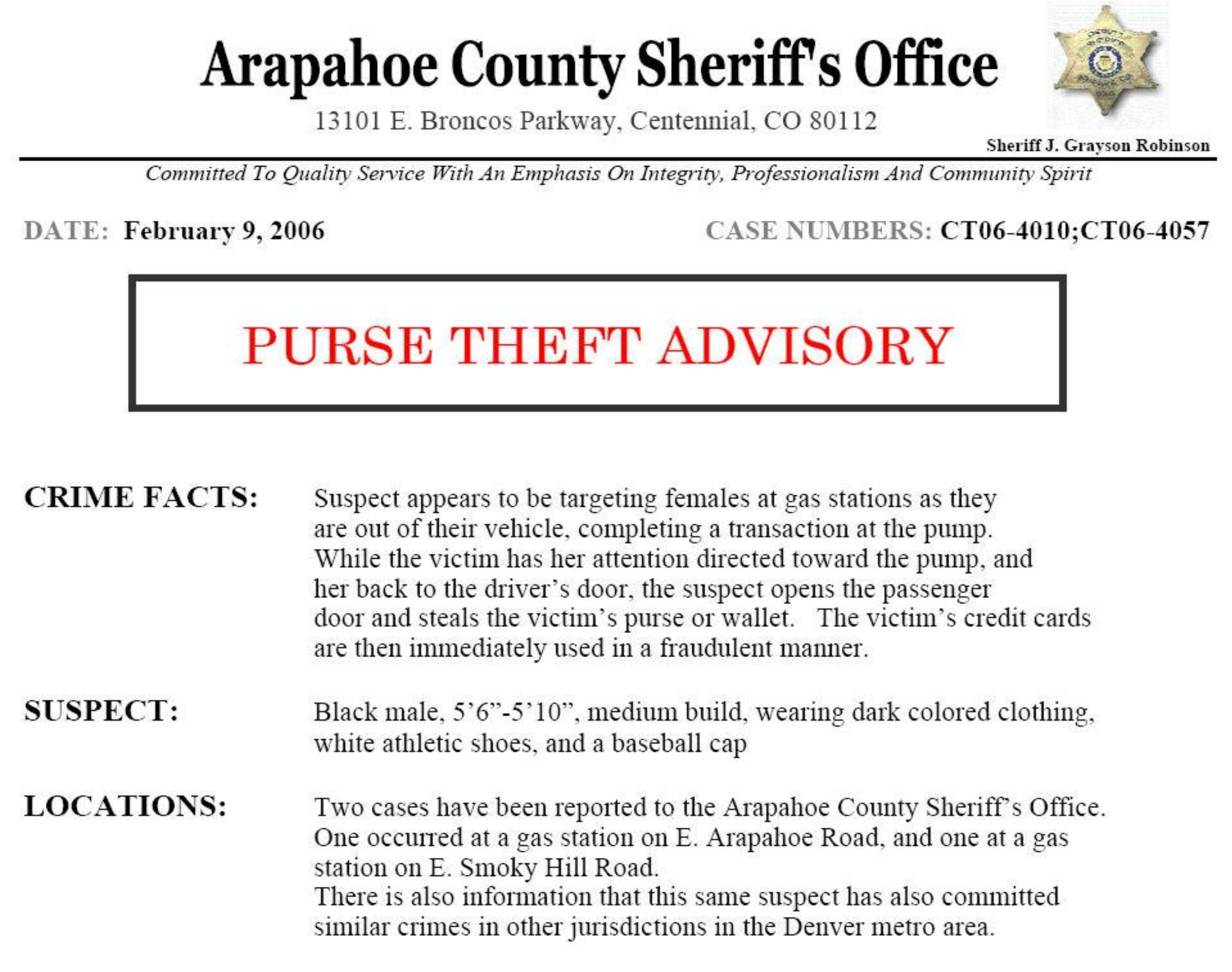
· Tell consumers there is a warrant for their arrest or an unpaid ticket or fine

· Tell consumers there is money waiting for them, but they must pay taxes before claiming it

· Threaten consumers with an arrest or legal action if they do not immediately wire money or provide a prepaid debit card

· Threaten consumers with liens and wage garnishments

Purse Theft Advisory



Arapahoe County Sheriff's Office

13101 E. Broncos Parkway, Centennial, CO 80112

Sheriff J. Grayson Robinson

Committed To Quality Service With An Emphasis On Integrity, Professionalism And Community Spirit

DATE: **February 9, 2006**

CASE NUMBERS: **CT06-4010;CT06-4057**

PURSE THEFT ADVISORY

CRIME FACTS: Suspect appears to be targeting females at gas stations as they are out of their vehicle, completing a transaction at the pump. While the victim has her attention directed toward the pump, and her back to the driver's door, the suspect opens the passenger door and steals the victim's purse or wallet. The victim's credit cards are then immediately used in a fraudulent manner.

SUSPECT: Black male, 5'6"-5'10", medium build, wearing dark colored clothing, white athletic shoes, and a baseball cap

LOCATIONS: Two cases have been reported to the Arapahoe County Sheriff's Office. One occurred at a gas station on E. Arapahoe Road, and one at a gas station on E. Smoky Hill Road.
There is also information that this same suspect has also committed similar crimes in other jurisdictions in the Denver metro area.

1_min_48_sec_Sliders_Steal_from_Cars_as_you_Pump_Gas

56_sec_gas_station_purse.mp4

Prevention Tips

Reduce your chances of being a victim of identity theft by remaining vigilant in all financial matters and taking precautions to protect your personal identifiers. Identity thieves can find ways to exploit your personal information in all avenues of your life. At work, at home, and on the Internet, your daily activities offer multiple opportunities for criminals to obtain your personal information.

Making yourself aware of the issues and information is the first step in safeguarding against identity theft. By making a slight change in your daily routine, you may be able to thwart a criminal from obtaining your personal information.

1_min_1sec_Thief Steals iPhone From baby

New Technology to Steal

3_min_45_sec_iPhone ATM PINhack.mp4

Your Daily Activities

- Ensure that your PIN numbers cannot be observed by anyone while you're utilizing an ATM or public telephone.
- Never leave receipts at bank machines, bank counters, trash receptacles or unattended gasoline pumps.
- Memorize your social security number and all passwords. Do not record them on any cards or on anything in your wallet or purse.

Your Mail

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post collection boxes or at your local post office.
- Contact your creditor or service provider if expected bills don't arrive.
- Never put your credit card or any other financial account number on a postcard or on the outside of an envelope.
- Beware of promotional solicitations through the mail or telephone that offer instant prizes or awards and seek to obtain your personal information or credit card numbers.

On the Internet

- Use caution when disclosing checking account numbers, credit card numbers, or other personal financial data at any web site or on-line service location unless you receive a secured authentication key from your provider.
- Don't email your personal data unless you use encryption technology
- Be very careful when giving information on unknown web sites, especially ones found in Spam e-mails
- Do not give out your checking account information on the internet, unless you are dealing directly with your bank's website.
- Make sure every transaction you engage in on the Internet is over a secure connection, you should see a lock in your browser window, as well as "https" in the browser window.
- Consider making a secondary, disposable online identity with an incorrect address, phone number using a "free" email account.

How to Protect Yourself

1. Guard your important personal information. A Social Security number is the prime example of this, although it's important to keep things like your birthdate, credit card number and driver's license number safe too. Only share your information with companies that you trust. And avoid carrying your Social Security card in your wallet — you have it memorized anyway (hopefully).
2. Shred private financial documents with a cross-cut shredder before recycling.
3. Avoid posting bills in your mailbox, where an identity thief can strike. Instead, place your outgoing mail in collection boxes or drop your bills and other mail at the post office.
4. Keep virus and spyware software up-to-date on your laptop and home computer and use firewall software for protection.
5. Use strong passwords to protect your accounts. And change your passwords frequently. You should also make sure you follow the advice of experts when data breaches happen – they can tell you whether you need to change your password, get credit monitoring or do more to protect your identity.
6. Get free annual copies of your credit reports from each of the major credit reporting agencies: Equifax, TransUnion and Experian.
7. Monitor your credit score. With Credit.com's free tools, you receive two free credit scores, updated every 14 days, plus expert tips on improving your credit. An unexpected change in your credit scores could mean an identity thief has opened an account in your name.

Note This came from an article that originally appeared on credit.com

http://www.clark.com/3-habits-fraud-victim

If You are a Victim

If you are a victim of identity theft, or believe you may be a victim, it is important that you take the following steps:

- Place a fraud alert on your credit reports and review your credit reports
- Place a security freeze on your credit reports.
- Close any accounts that have been tampered with or opened fraudulently.
- File a police report and ask for a copy for your records
- File a complaint with the Federal Trade Commission and the Attorney General's Office.
- Write down the name of anyone you talk to, what s/he told you, and the date of the conversation.
- Follow-up in writing with all contacts you have made about the identity theft on the phone or in person. Use certified mail, return receipt requested, for all correspondence regarding identity theft.
- Keep all copies of all correspondence or forms relating to identity theft.
- Keep the originals of supporting documentation, like police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved. If it happens again, you will be glad you did.

A Final Word

Think!

Comments?