

Identity Theft

How to Avoid it

Saturday October 17, 2015

Hewie Poplock, Vice-President APCUG

hpoplock@apcug.org



What is Identity Theft?

According to the non-profit Identity Theft Resource Center, identity theft is subdivided into four categories:

1. Financial Identity Theft (using another's identity to obtain goods and services)
2. Criminal Identity Theft (posing as another when apprehended for a crime)
3. Identity Cloning (using another's information to assume his or her identity in daily life)
4. Business/Commercial Identity Theft (using another's business name to obtain credit)

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.

Federal Trade Commission Website

FEDERAL TRADE COMMISSION

ESPAÑOL

CONSUMER INFORMATION

Search

MONEY & CREDIT

HOMES & MORTGAGES

HEALTH & FITNESS

JOBS & MAKING MONEY

PRIVACY & IDENTITY

Limiting Unwanted Calls and Emails

Computer Security

Kids' Online Safety

Protecting Your Identity

Repairing Identity Theft

BLOG

VIDEO & MEDIA


SCAM ALERTS

Privacy & Identity

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.

Recover from Identity Theft



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.

Computer 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.


Kids' Online Safety

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.

Protecting Your Identity

Keeping your important papers secure, shredding documents with sensitive information before you put them in the trash, and limiting the personal information you carry with you are among the ways you can protect your identity. Find additional tips to reduce your risk of identity theft, including how and when to order your free credit report.

Related Items



What is Identity Theft?

• Immediate Steps to Repair Identity Theft

• Credit Freeze FAQs

• How to Keep Your Personal Information Secure

• Spam

• Kids and Socializing Online

Recent Blog Posts

• Hack Attack: Health insurer's customer information stolen
February 5, 2015

• Technology tips for domestic violence and stalking victims
February 5, 2015

• Hotel Wi-Fi: Weigh the risk
February 4, 2015

<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.
- RFID – (Radio-frequency Identification) wireless credit card theft
- 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.

Ways Identity Theft Can Occur

Thieves:

- 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)

Ways Identity Theft Can Occur

Thieves (continued):

- 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.

5 Ways to Steal an ID

Video

2_min_41sec_5ways_to_steal_id

Misconceptions

Clarifying Four Key Misperceptions Surrounding Identity Fraud

Misperception #1: "Consumers are helpless to protect themselves"

Misperception #2: "Consumers bear the brunt of the financial losses from identity fraud"

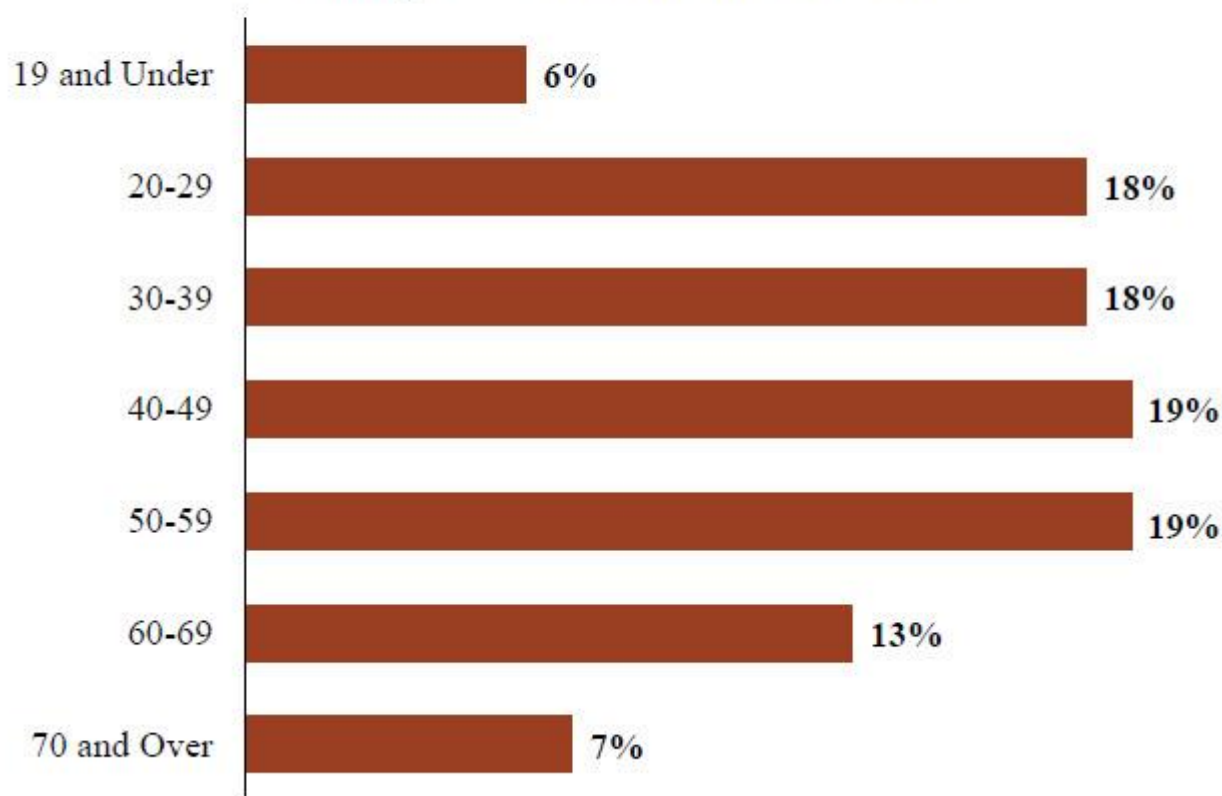
Misperception #3: "Seniors are most frequent targets of fraud operators"

Misperception #4: "Internet use increases the risks of identity fraud"

ID Theft by Age 2014

Consumer Sentinel Network Identity Theft Complaints by Victims' Age¹

January 1 – December 31, 2014



ID Theft by Age 2012-2014

Consumer Sentinel Network Identity Theft Complaints by Victims' Age *Calendar Years 2012 through 2014*

Consumer Age	CY - 2012		CY - 2013		CY - 2014	
	Complaints	Percentages ¹	Complaints	Percentages ¹	Complaints	Percentages ¹
19 and Under	16,045	6%	11,875	6%	12,062	6%
20-29	57,178	21%	39,058	20%	37,568	18%
30-39	52,312	19%	37,777	19%	38,714	18%
40-49	49,002	18%	35,241	18%	39,649	19%
50-59	45,121	17%	33,823	17%	41,020	19%
60-69	30,287	11%	24,156	12%	27,799	13%
70 and Over	21,873	8%	16,869	8%	15,886	7%
Total Reporting Age	271,818		198,799		212,698	

¹Percentages are based on the total number of victims reporting their age in CSN identity theft complaints for each calendar year: CY-2012 = 271,818; CY-2013 = 198,799; and CY-2014 = 212,698. Of the consumers who contacted the FTC, 64% reported their age in CY-2014, 69% in CY-2013 and 74% in CY-2012.



1

CHILDREN ARE
TARGETED
**35 TIMES
MORE**
OFTEN THAN
ADULTS



2

PEOPLE WITH
PERSONAL
INFORMATION
**ON THEIR
SOCIAL MEDIA
PROFILE**



3

SMARTPHONE
OWNERS
HAVE A **33%
HIGHER RATE
OF ID FRAUD**
THAN THAT OF
GENERAL PUBLIC



7

HOUSEHOLDS
WITH INCOMES
GREATER THAN
\$150,000
ARE **73% MORE LIKELY**
TO BE VICTIMIZED



6

VICTIMS OF DATA
BREACHES
ARE **9.5 TIMES
MORE LIKELY TO BE
A VICTIM OF
ID FRAUD**



5

MORE OFTEN
**COLLEGE
STUDENTS**
HAVE GOOD, CLEAN
CREDIT SCORES,
WHICH MAKE THEM
IDEAL TARGETS



4

**25% OF PEOPLE
AFFECTED BY
FRAUD, ANNUALLY ARE
DEAD PEOPLE
(YES, DEAD!)**

Florida Ranks as Top State In U.S. For ID Theft



Florida Ranks as Top State In U.S. For ID Theft

- In a state-by-state comparison for fraud, Florida tops the list: in 2014, 200,392 complaints of fraud were reported in the state. For every 100,000 people, that's 1007.3 reports — the highest rate in the country. The number two spot went to Georgia, which notched 777.7 complaints per 100,000.
- If we're just talking identity fraud, Florida again tops a state-by-state comparison with 37,059 complaints in 2014.
- That equates to 186.3 reports per 100,000 people. Coming in second: Washington, with 154.8 complaints.

Consumer Sentinel Network State Complaint Rates

January 1 – December 31, 2014

Fraud & Other Complaints

Rank	Consumer State	Complaints Per 100,000	
		Population ¹	Complaints
1	Florida	1,007.3	200,392
2	Georgia	777.7	78,526
3	Nevada	773.2	21,952
4	Delaware	769.2	7,197
5	Michigan	749.2	74,244
6	Maryland	675.5	40,369
7	Texas	647.2	174,468
8	California	644.6	250,138
9	New Jersey	598.9	53,535
10	Colorado	598.6	32,060
11	Virginia	594.9	49,537
12	Rhode Island	589.4	6,219
13	Alabama	574.2	27,847
14	Tennessee	570.2	37,347
15	New Hampshire	562.6	7,464
16	Arizona	562.1	37,836
17	Massachusetts	554.8	37,422
18	Pennsylvania	544.7	69,655
19	Louisiana	538.9	25,059
20	South Carolina	534.2	25,816
21	Missouri	516.3	31,304
22	New York	514.0	101,497
23	Washington	511.6	36,127
24	Connecticut	509.1	18,312
25	Wyoming	508.1	2,968
26	North Carolina	507.9	50,504
27	Ohio	506.3	58,704
28	New Mexico	506.1	10,556
29	Oregon	505.5	20,069
30	Illinois	473.9	61,058
31	West Virginia	466.6	8,634
32	Arkansas	465.2	13,800
33	Indiana	464.7	30,636
34	Idaho	456.8	7,466
35	Kentucky	451.1	19,907
36	Montana	444.5	4,550
37	Maine	444.3	5,909
38	Mississippi	443.4	13,276
39	Oklahoma	436.5	16,926
40	Kansas	432.8	12,569
41	Minnesota	423.0	23,083
42	Wisconsin	422.4	24,321
43	Hawaii	419.6	5,957
44	Nebraska	414.9	7,807
45	Alaska	408.7	3,011
46	Utah	389.8	11,471
47	Vermont	389.7	2,442
48	Iowa	365.4	11,354
49	South Dakota	348.6	2,974
50	North Dakota	334.4	2,473

Identity Theft Complaints

Rank	Victim State	Complaints Per 100,000	
		Population ¹	Complaints
1	Florida	186.3	37,059
2	Washington	154.8	10,930
3	Oregon	124.6	4,946
4	Missouri	118.7	7,195
5	Georgia	112.7	11,384
6	Michigan	104.3	10,338
7	California	100.5	38,982
8	Nevada	100.2	2,846
9	Arizona	96.0	6,460
10	Maryland	95.9	5,734
10	Texas	95.9	25,843
12	Illinois	95.6	12,317
13	Colorado	85.5	4,579
14	Connecticut	85.4	3,071
15	Arkansas	83.6	2,481
16	Pennsylvania	81.7	10,446
17	New York	80.8	15,959
18	Mississippi	80.5	2,409
19	New Jersey	79.9	7,144
20	Ohio	79.0	9,161
21	Delaware	78.1	731
22	Alabama	77.7	3,770
23	New Mexico	77.2	1,611
24	Tennessee	76.2	4,993
25	Massachusetts	75.8	5,116
26	Wisconsin	74.4	4,283
27	Louisiana	73.8	3,430
27	North Carolina	73.8	7,334
29	Alaska	73.6	542
30	South Carolina	73.3	3,540
31	Virginia	71.1	5,921
32	Oklahoma	68.5	2,656
33	Indiana	68.2	4,498
34	Rhode Island	66.2	699
35	Kansas	65.2	1,892
36	Vermont	64.2	402
37	West Virginia	61.4	1,136
38	Minnesota	59.2	3,229
39	Idaho	58.9	962
40	Montana	57.2	585
41	New Hampshire	54.7	726
42	Utah	53.9	1,586
43	Kentucky	53.4	2,358
44	Maine	52.1	693
45	Wyoming	49.1	287
46	Nebraska	48.6	914
47	Iowa	48.5	1,506
48	North Dakota	43.1	319
49	Hawaii	40.9	580
50	South Dakota	36.3	310

¹Per 100,000 unit of population estimates are based on the 2014 U.S. Census population estimates (Table NST-EST2014-01 -- Annual Estimates of the Resident Population for the United States, Regions, States, and Puerto Rico: April 1, 2010 to July 1, 2014). Numbers for the District of Columbia are: Fraud and Other = 6,605 complaints and 1,002.4 complaints per 100,000 population; Identity Theft = 941 victims and 142.8 victims per 100,000 population.

Note: In calculating the State and Metropolitan Areas rankings, we excluded 20 state-specific data contributors' complaints (the Hawaii Office of Consumer Protection, the Montana, North Carolina and Oregon Departments of Justice, the South Carolina Department of Consumer Affairs, the Tennessee Division of

Largest Metropolitan Areas Ranking for Identity Theft – Related Consumer Complaints¹

January 1 – December 31, 2014

Rank	Metropolitan Area	Complaints Per	
		Complaints	100,000 Population ¹
1	Miami-Fort Lauderdale-West Palm Beach, FL Metropolitan Statistical Area	18,428	316.2
2	Seattle-Tacoma-Bellevue, WA Metropolitan Statistical Area	7,473	207.0
3	St. Louis, MO-IL Metropolitan Statistical Area	5,724	204.4
4	Tallahassee, FL Metropolitan Statistical Area	706	189.1
5	Naples-Immokalee-Marco Island, FL Metropolitan Statistical Area	586	172.5
6	Olympia-Tumwater, WA Metropolitan Statistical Area	418	159.3
7	Portland-Vancouver-Hillsboro, OR-WA Metropolitan Statistical Area	3,685	159.2
8	Pueblo, CO Metropolitan Statistical Area	252	156.1
9	Jacksonville, FL Metropolitan Statistical Area	2,156	154.6
10	Detroit-Warren-Dearborn, MI Metropolitan Statistical Area	6,522	151.9
11	Cape Coral-Fort Myers, FL Metropolitan Statistical Area	988	149.4
12	Port St. Lucie, FL Metropolitan Statistical Area	650	148.4
13	Lakeland-Winter Haven, FL Metropolitan Statistical Area	908	145.7
14	Salem, OR Metropolitan Statistical Area	567	141.6
15	Atlanta-Sandy Springs-Roswell, GA Metropolitan Statistical Area	7,809	141.4
15	Beckley, WV Metropolitan Statistical Area	176	141.4
17	Orlando-Kissimmee-Sanford, FL Metropolitan Statistical Area	3,124	137.8
17	Tampa-St. Petersburg-Clearwater, FL Metropolitan Statistical Area	3,956	137.8
19	Stockton-Lodi, CA Metropolitan Statistical Area	915	129.9
20	Vallejo-Fairfield, CA Metropolitan Statistical Area	549	129.2
21	Deltona-Daytona Beach-Ormond Beach, FL Metropolitan Statistical Area	769	128.0
22	Columbus, GA-AL Metropolitan Statistical Area	404	127.6
23	Milwaukee-Waukesha-West Allis, WI Metropolitan Statistical Area	2,002	127.5
24	Memphis, TN-MS-AR Metropolitan Statistical Area	1,650	123.0
25	Longview, WA Metropolitan Statistical Area	124	121.7
26	The Villages, FL Metropolitan Statistical Area	130	121.4
27	Dallas-Fort Worth-Arlington, TX Metropolitan Statistical Area	8,158	119.8
28	Sebastian-Vero Beach, FL Metropolitan Statistical Area	170	119.7
29	Mount Vernon-Anacortes, WA Metropolitan Statistical Area	140	117.8
30	Fresno, CA Metropolitan Statistical Area	1,121	117.3
31	Flint, MI Metropolitan Statistical Area	482	116.0
32	Gainesville, FL Metropolitan Statistical Area	312	115.4
33	Ocala, FL Metropolitan Statistical Area	389	115.3
34	Montgomery, AL Metropolitan Statistical Area	425	113.8
35	Dothan, AL Metropolitan Statistical Area	167	113.1
36	Bremerton-Silverdale, WA Metropolitan Statistical Area	287	113.0
37	Houston-The Woodlands-Sugar Land, TX Metropolitan Statistical Area	7,076	112.1
38	San Francisco-Oakland-Hayward, CA Metropolitan Statistical Area	5,060	112.0
39	North Port-Sarasota-Bradenton, FL Metropolitan Statistical Area	817	111.5
40	Los Angeles-Long Beach-Anaheim, CA Metropolitan Statistical Area	14,397	109.6
41	Palm Bay-Melbourne-Titusville, FL Metropolitan Statistical Area	602	109.3
42	Modesto, CA Metropolitan Statistical Area	568	108.1
43	Jackson, MS Metropolitan Statistical Area	621	107.7
44	Laredo, TX Metropolitan Statistical Area	282	107.4
45	Waterloo-Cedar Falls, IA Metropolitan Statistical Area	181	106.8
46	Racine, WI Metropolitan Statistical Area	206	105.6
47	Pittsburgh, PA Metropolitan Statistical Area	2,479	105.0
48	Chicago-Naperville-Elgin, IL-IN-WI Metropolitan Statistical Area	9,992	104.8

'Farcing' overtaking 'phishing' as online identity theft threat

- Scammers have discovered social media.
- To them, email phishing scams are so 2009.
- Really aggressive identity thieves are now using social media sites like Facebook, Twitter and LinkedIn to ensnare victims. It turns out it's easier and a lot more lucrative.
- Social media users are always getting friend requests. Most often it's someone from the user's circle of friends. But getting a friend request from a friend-of-a-friend is not uncommon.
- Assuming that person is who they say they are, without confirming it, is dangerous, says Arun Vishwanath, associate professor of communication at the University of Buffalo. You could fall victim to what's being called “farcing,” exposing dozens of your friends and contacts for good measure.



Video

13_sec_ShoppingCart purse-snatching

Video

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

2014 Data Breaches

- **There were 3,014 incidents reported during 2014 exposing 1.1 billion records.**
- Four Hacking incidents alone exposed a combined 647 million records.
- **A single act of Fraud exposed 104 million records.**
- The Business sector accounted for 52.9% of reported incidents, followed by Government (15.5%), Unknown (13.2%), Medical (9.6%), and Education (8.8%).
- The Business sector accounted for 55.1% of the number of records exposed, followed by Unknown (25.9%), and Government (17.9%).
- **67.7% of reported incidents were the result of Hacking, which accounted for 83.3% of the exposed records.**
- Fraud accounted for 14.3% of the exposed records, but represented just 4.3% of the reported incidents.
- Five of 2014 incidents have secured a place on the Top 10 All Time Breach List.
- The number of reported incidents tracked by Risk Based Security has exceeded 14,400 exposing over 3.6 billion records.

Data Breaches 2014

Identity Theft Resource Center

2014 Breach List: Breaches: **783** Exposed: **85,611,528**

<http://www.idtheftcenter.org/>

Data Breaches 2015



Identity Theft Resource Center

2015 Data Breach Stats



2015 Breaches Identified by the ITRC as of: 10/13/2015

Total Breaches: 606

Records Exposed: 175,492,082

<http://www.idtheftcenter.org/>

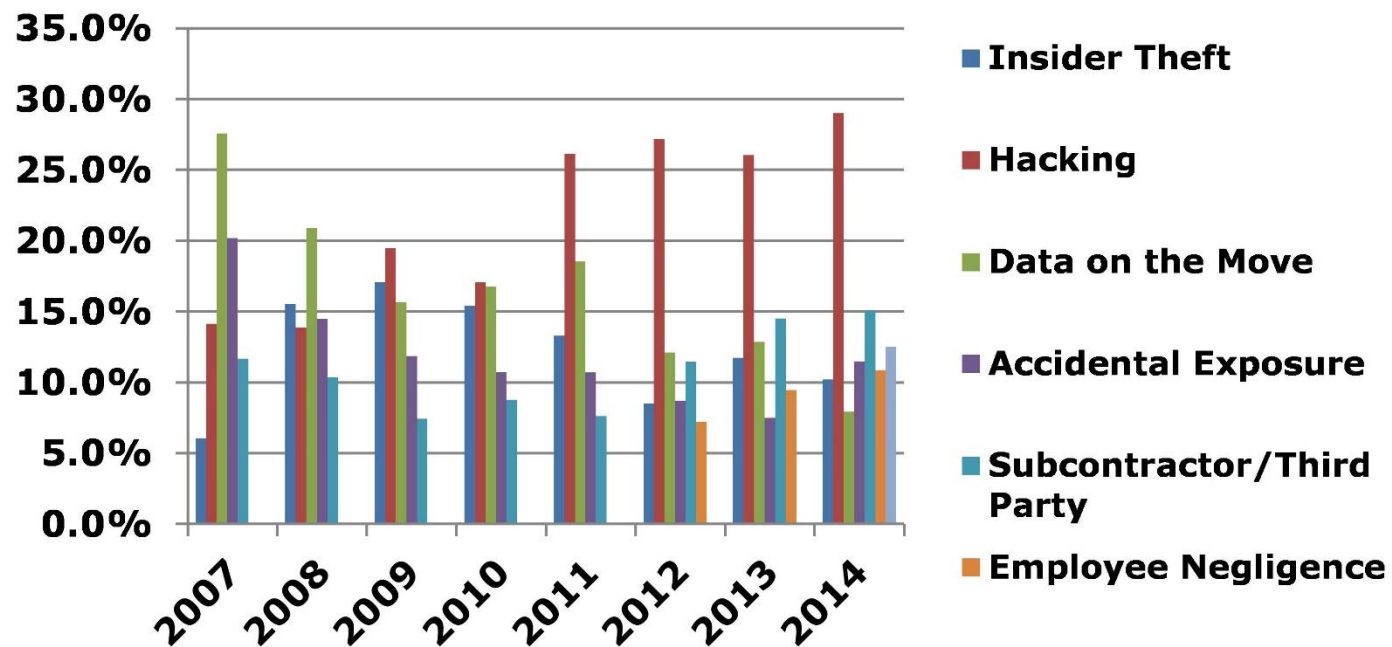
Data Breaches 2005 - 2014

Number of breaches = 5,029

Number of Records = 677,749,785

Types of Breaches

Cause/Type of Breach (2007 - 2014)



Types of Breaches

- Over the years, **hacking** has been a primary cause of data breach incidents, leading to an 8-year average of 21.7 percent.
- **Data on the Move**, a leading cause of breaches in 2007 and 2008, ranks second with an average of 15.9 percent. (This category includes storage devices or laptops lost in transit.)
- **Insider theft** and **Accidental Exposure** follow at just over 12 percent, and **Subcontractor/Third Party** follows at 11.2 percent.

Category Summary



Identity Theft Resource Center

2015 Data Breach Category Summary



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

Report Date: 10/6/2015

Page 1 of 1

Totals for Category: Banking/Credit/Financial	# of Breaches: 56 % of Breaches: 9.5%	# of Records: 5,012,381 %of Records: 2.9%
Totals for Category: Business	# of Breaches: 230 % of Breaches: 38.9	# of Records: 16,004,036 %of Records: 9.1%
Totals for Category: Educational	# of Breaches: 49 % of Breaches: 8.3%	# of Records: 754,100 %of Records: 0.4%
Totals for Category: Government/Military	# of Breaches: 45 % of Breaches: 7.6%	# of Records: 33,802,728 %of Records: 19.3%
Totals for Category: Medical/Healthcare	# of Breaches: 211 % of Breaches: 35.7	# of Records: 119,870,643 %of Records: 68.3%
Totals for All Categories:	# of Breaches: 591 % of Breaches: 100.0	# of Records: 175,443,888 %of Records: 100.0%

2015 Breaches Identified by the ITRC as of: 10/6/2015

Total Breaches: 591
Records Exposed: 175,443,888

Category Stats



Identity Theft Resource Center



2015 Data Breach Stats

How is this report produced? What are the rules? See last page of report for details. Report Date: 10/6/2015

Page 9 of 19

ITRC20150122-08	American Airlines	TX	Business	Yes - Unknown #	Unknown
ITRC20150122-07	United Airlines	IL	Business	Yes - Unknown #	Unknown
ITRC20150122-06	Law Offices of David A. Krausz, P.C.	CA	Business	Yes - Unknown #	Unknown
ITRC20150122-05	ValuePetSupplies.com / Piech Sales Company	TN	Business	Yes - Unknown #	Unknown
ITRC20150122-04	Barbecue Renew / Grillparts.com	FL	Business	Yes - Unknown #	Unknown
ITRC20150122-03	Six Red Marbles, LLC	MA	Business	Yes - Unknown #	Unknown
ITRC20150121-09	Rentrak Corporation	OR	Business	Yes - Unknown #	Unknown
ITRC20150121-05	Polish Falcons of America	PA	Business	Yes - Unknown #	Unknown
ITRC20150121-03	Allied-Barton	PA	Business	Yes - Unknown #	Unknown
ITRC20150121-01	Asset Marketing Services / GovMint.com	MN	Business	Yes - Unknown #	Unknown
ITRC20150109-01	Libbey Inc.	OH	Business	Yes - Unknown #	Unknown
ITRC20150107-03	Art of Tea	CA	Business	Yes - Unknown #	Unknown
ITRC20150107-01	Fast Forward Academy	FL	Business	Yes - Unknown #	Unknown
ITRC20150105-02	La Jolla Group	CA	Business	Yes - Unknown #	Unknown

Totals for Category: **Business**

of Breaches: 230

of Records:

16,004,036

% of Breaches: 38.9

% of Records:

9.1%

Category: Educational

ITRC Breach ID	Company or Agency	State	Breach Category	Records Exposed?	Exposed # of Records
ITRC20150929-12	North Oldham High School	KY	Educational	Yes - Published #	2,800
ITRC20150922-07	Hackers breach Commack High School computer syst	NY	Educational	Yes - Unknown #	Unknown

Data Breach

5 HACKERS CHARGED IN LARGEST DATA-BREACH SCHEME IN U.S.

By David Voreacos - Jul 25, 2013 9:23 AM ET

Four Russians and a Ukrainian were charged for their role in the largest hacking and data breach scheme in U.S. history, according to Paul Fishman, the U.S. attorney in New Jersey.

The five conspired in a “worldwide scheme that targeted major corporate networks, stole more than 160 million credit card numbers and resulted in hundreds of millions of dollars in losses,” Fishman said today in a statement. The men worked with Albert Gonzalez, a hacker serving 20 years in prison, according to the indictment unsealed in federal court in New Jersey.

The men operated “a prolific hacking organization” that “penetrated the secure computer networks of several of the largest payment-processing companies, retailers and financial institutions in the world,” according to the indictment. They are accused of stealing user names and passwords, personal identification information, and credit and debit card numbers.

Bloomberg
LAW

PRACTICE CENTERS

PRODUCT FEATURES



<http://about.bloomberglaw.com/legal-news/5-hackers-charged-in-largest-data-breach-scheme-in-u-s/>

Passwords

SplashData, which makes password management applications, has released its annual list of the 25 worst passwords based on files containing over 3.3. million passwords leaked in 2014.

Here is the full list:

Worst Passwords

- | | | |
|--------------|--------------|--------------|
| 1. 123456 | 10. football | 19. master |
| 2. password | 11. 1234567 | 20. michael |
| 3. 12345 | 12. monkey | 21. superman |
| 4. 12345678 | 13. letmein | 22. 696969 |
| 5. qwerty | 14. abc123 | 23. 123123 |
| 6. 123456789 | 15. 111111 | 24. batman |
| 7. 1234 | 16. mustang | 25. trustno1 |
| 8. baseball | 17. access | |
| 9. dragon | 18. shadow | |

Password DOs

- Do vary it up, using a different password for each online account
- Do get complicated, with randomized numbers to make things complicated for cyber criminals
- Do change your passwords every few months
- Do stay off the list. If it's on the list of common passwords above, don't use it for your password!
- Capital letters, symbols, underscores, oh my! Adding in these extra elements can help make any password complex

Password Don'ts

- Don't use a string of consecutive numbers or letters, especially starting with "1" or "a"
- Don't include the name of the application (i.e., adobe123)
- Don't use your name, address or company information
- Don't save your passwords within a document on your computer
- If the word seems like something your kindergartener could guess – keep thinking!

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.

Video

2_min_23_sec_skimmers_hernando_WFTS-TV

Older Skimmers



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.

Newer Skimmers



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
- Check for Tape over Panel Edge

Video

3_min_45_sec_iPhone ATM PINhack

Tuesday, March 17, WWSB ABC7
<http://www.mysuncoast.com>



TAMPA, Fla -- The Florida Department of Agriculture and Consumer Services is warning drivers about credit card skimmers. In the past week, inspectors have removed six skimmers from gas station pumps across the Tampa Bay area.

The devices are placed illegally on gas station debit or credit card machines. Criminals use the devices to steal debit or credit card information from consumers and use the information to make purchases in someone else's name.

The Florida Department of Agriculture and Consumer Services' law enforcement officers and gas station inspectors worked with the Pasco County Sheriff's Office, Pinellas County Sheriff's Office, the Florida Department of Law Enforcement and the Secret Service to inspect 640 gas stations in Pasco, Pinellas and Hillsborough counties last week.

Five skimmers were found in Hillsborough County, and one was located in Pasco County.

Tuesday, March 17, WWSB ABC7
<http://www.mysuncoast.com>



Here's what consumers can do to avoid skimmers at gas stations:

- Pay in cash inside the store to ensure the credit card information stays safe.
- Check to make sure the gas pump dispenser cabinet is closed and has not been tampered with. Many stations are now putting a piece of security tape over the cabinet to ensure it has not been opened by unauthorized individuals.
- Try to use a gas pump closer to the front of the store. Thieves often place skimmers at the gas pumps farther away from the store so they are not noticed as quickly.
- Use a credit card instead of a debit card. Credit cards have better fraud protection, and the money is not deducted immediately from an account.
- If using a debit card at the pump, choose to run it as a credit card instead of a PIN number in. That way, the PIN number is safe.
- Monitor bank accounts regularly to spot any unauthorized charges.

Tuesday, March 17, WWSB ABC7
<http://www.mysuncoast.com>



Here's what consumers can do to avoid skimmers at gas stations:

- Consumers who suspect their credit card number has been compromised should report it immediately to authorities and their credit card company.
- Consumers who believe fraud has taken place can contact the department's consumer protection and information hotline at **1-800-HELP-FLA (435-7352)** or, for Spanish speakers, 1-800-FL-AYUDA (352-9832). For more information about the Florida Department of Agriculture and Consumer Services, visit **<http://www.FreshFromFlorida.com>** .

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.



RFID & EMV



EMV

What is an EMV credit card?

EMV Chip The small gold chip found in many credit cards is most often referred to as an EMV chip. Cards containing this chip are known as EMV cards, as well as “chip-and-signature,” “chip-and-pin,” or “smart” cards. The name “EMV” refers to the three originators of chip-enabled cards: Europay, MasterCard, and Visa. EMV chips are now the global standard for credit card security.

RFID & EMV

- Late night infomercials hawk aluminum wallets and other gadgets that claim to block thieves from zapping your account details right from your purse or pocket. You don't need those to protect your credit card information. Unlike other, stronger chips based on RFID technology, EMV chips in contactless credit cards work only in very short range from payment terminals.
- Even if a thief managed to nab your card's contents with a suitcase-sized mobile scanner, he or she would only have access to its raw codes, not your actual account details. Trying to use a copied code would result in a declined transaction and a fraud investigation from your card issuer.

FBI Warning

New Microchip-Enabled Credit Cards May Still Be Vulnerable to Exploitation by Fraudsters

By October 2015, many U.S. banks will have replaced hundreds of millions of traditional credit and debit cards, which rely on data stored on magnetic strips, with new payment cards containing a microchip known as an EMV chip. While EMV cards offer enhanced security, the FBI is warning law enforcement, merchants, and the general public that no one technology eliminates fraud and cybercriminals will continue to look for opportunities to steal payment information.

Released October 13, 2015

<http://www.ic3.gov/media/2015/151008.aspx>

The Bad Guys Do Get Caught



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



Florida Law



The screenshot shows the official website of the Florida Department of Agriculture and Consumer Services. The header includes the department's name and a search bar. A navigation menu lists various services like Home, Pay Online, About, Divisions & Offices, Forms & Publications, News & Events, and Contact. A breadcrumb trail indicates the current location: Home > Divisions & Offices > Consumer Services > Consumer Resources > Consumer Protection > Scams and Fraud > Security Freeze - Credit Report. The left sidebar features the department's seal, the Commissioner's name (Adam H. Putnam), and a list of links for Scams and Fraud, including Concealed Weapon, License Fraud, Little Black Book of Scams, Phishing, Mortgage Assistance, Relief Scams, Travel Fraud, Security Freeze - Credit Report (highlighted), Return Call Scam, and Oil Spill Scams. The main content area is titled "Security Freeze - Credit Report" and "Freeze Frequently Asked Questions". It defines a security freeze, explains how to place one, and lists the agencies involved (Equifax, Experian, TransUnion).

Florida Department of Agriculture and Consumer Services

Search **SEARCH**

[Home](#) [Pay Online](#) [About](#) [Divisions & Offices](#) [Forms & Publications](#) [News & Events](#) [Contact](#)

You are here: [Home](#) > [Divisions & Offices](#) > [Consumer Services](#) > [Consumer Resources](#) > [Consumer Protection](#) > [Scams and Fraud](#) > [Security Freeze - Credit Report](#)

Security Freeze - Credit Report

Freeze Frequently Asked Questions

What is a security freeze? [\[s.501.005\(1\)\]](#)

A security freeze is a notice that is placed in a consumer report (on request of the consumer) that prohibits a consumer reporting agency (such as [Equifax](#), [Experian](#) and [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.

How can I place a security freeze on my credit files? [\[s.501.005\(2\),\(4\)\]](#)

In order to place a security freeze on your credit files, you must request the freeze with each of the three major credit reporting agencies ([Equifax](#), [Experian](#) and [TransUnion](#)) and any other credit reporting agency. All agencies are required to allow consumers to request security freezes via certified mail, however additional methods may be available. Please check with each credit reporting agency regarding its policies concerning security freezes.

Adam H. Putnam
Commissioner

Scams and Fraud

- [Concealed Weapon](#)
- [License Fraud](#)
- [Little Black Book of Scams](#)
- [Phishing](#)
- [Mortgage Assistance](#)
- [Relief Scams](#)
- [Travel Fraud](#)
- [Security Freeze - Credit Report](#)**
- [Return Call Scam](#)
- [Oil Spill Scams](#)

411 Wireless

- 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

On Line Shopping

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 - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=0

ShopSafe Use my: perks Advantage Gold MasterCard er HELP

Numbers Purchases

Create a New ShopSafe Number View All Active ShopSafe Numbers

Spending limit for this number: \$ 50.00

Months this number will be valid: 2

Create Number

Bank of America Access Online Banking

Internet | Protected Mode: On 100%

ShopSafe - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=0

ShopSafe Use my: perks Advantage Gold MasterCard er HELP

Numbers Purchases

Your New ShopSafe Number View All Active ShopSafe Numbers

5327 0787 4236 0778

Spending Limit \$50.00 Valid Thru 04/08 CVC2 (Security Code) [REDACTED]

Increase ShopSafe Limits

Cardholder Name [REDACTED]

MasterCard

Bank of America Access Online Banking

Internet | Protected Mode: On 100%

ShopSafe - Windows Internet Explorer
https://www.mbnashopsafe.com/NASApp/Athena/HTMLServlet?pageid=0

ShopSafe Use my: perks Advantage Gold MasterCard er HELP

Numbers Purchases

Your New ShopSafe Number View All Active ShopSafe Numbers

5327 0787 4236 0778

Spending Limit \$50.00 Valid Thru 04/08 CVC2 (Security Code) [REDACTED]

Increase ShopSafe Limits

Cardholder Name [REDACTED]

MasterCard

Bank of America Access Online Banking

Internet | Protected Mode: On 100%

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 formerly DoNotTrackMe, which we've covered here. They're a browser extension and mobile app, and they've since made many updates to the service. One of the most appealing features is credit card masking, which allows you to buy items without actually giving out any information. The feature is free for thirty days, but then it costs \$4.99 a month.



[Home](#)[News](#)[Travel](#)[Money](#)[Sports](#)[Life](#)[Technology](#)[Products](#)[Science & Space](#)[Gaming](#)[Wi-Fi Center](#)

Photocopiers with disk drives could be used for ID theft

Updated 245d ago | [Comment](#)

| [Recommend](#)

4

[E-mail](#) | [Save](#) | [Print](#)

By May Wong, Associated Press

SAN JOSE, Calif. — Consumers are bombarded with warnings about identity theft. Publicized threats range from mailbox thieves and lost laptops to the higher-tech methods of e-mail scams and corporate data invasions.

Now, experts are warning that photocopiers could be a culprit as well.



Most digital copiers manufactured in the past five years have 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.



04 Data Breach at Health Insurer Anthem Could Impact Millions

FEB 15

Anthem Inc., the nation's second largest health insurer, disclosed Wednesday that hackers had broken into its servers and stolen Social Security numbers and other personal data from all of its business lines. Given the company's size, this breach could end up impacting tens of millions of Americans.

Anthem didn't specify how many consumer records may have been breached, but it did say all of the company's business units are affected. The **figures from Anthem's Web site** offer a glimpse at just how big this breach could be: "With nearly 69 million people served by its affiliated companies including more than 37 million enrolled in its family of health plans, Anthem is one of the nation's leading health benefits companies."

The Anthem logo, featuring the word "Anthem" in a blue serif font, underlined with a blue line, and a small registered trademark symbol (®) to the right.

Theft after Death

ID theft ruins lives, even after death, Beach family finds

Posted to: [Crime](#) [News](#) [Virginia Beach](#) [Login or register](#) to post comments



1 OF 2 PHOTOS: Gregory Welch, 18, died in a car crash on Shore Drive on Feb. 14. His parents say his identity likely was stolen after his death and was used to submit a falsified tax return. (Family photo)

[View second photo | Download photos](#)

By [Kathy Adams](#)
The Virginian-Pilot
© September 10, 2013

VIRGINIA BEACH

Virginia and Kenneth Welch, like many parents, never thought about having to bury their 18-year-old son, close his accounts, settle what little there was of the community college student's estate.

They certainly never thought about checking Gregory Welch's credit report after his death.

But when the still-grieving parents went to file their son's tax return a few months after his Valentine's Day death in a Shore Drive crash, they got a surprise: someone had beaten them to it. They contacted the Internal Revenue Service and, later, the U.S. Attorney's Office for the Eastern District of Virginia, and learned their son had been a victim

<http://hamptonroads.com/2013/09/id-theft-ruins-lives-even-after-death-beach-family-finds>

Children & ID Theft

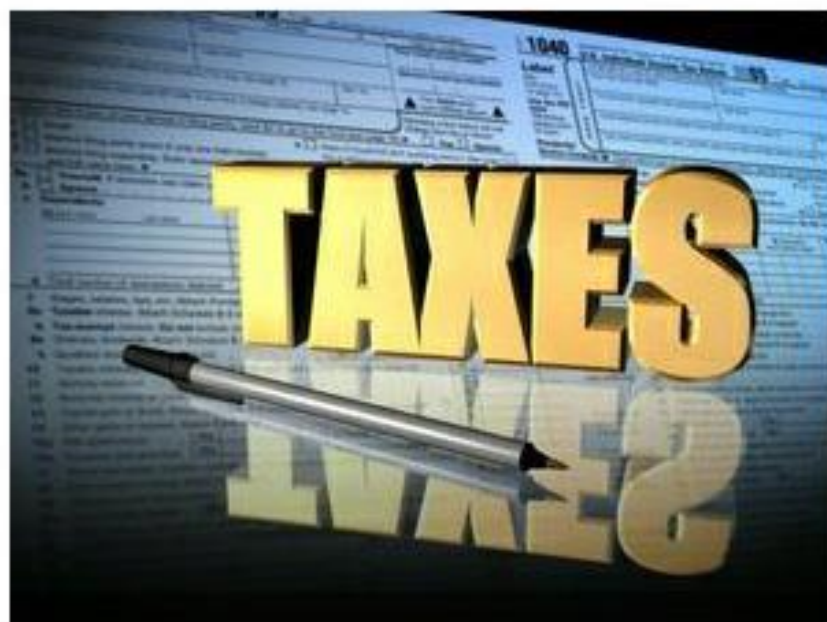
Protect your children

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.



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.

Video

1_min_48_sec_Sliders_Steal_from_Cars_as_you_Pump_Gas

ATTORNEY GENERAL
PAM BONDI
FLORIDA OFFICE OF THE ATTORNEY GENERAL



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.

Video

1_min_1sec_Thief Steals iPhone From baby

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.

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!

Questions?

Hewie Poplock

Vice-President APCUG

hpoplock@apcug.org



**An International
Association of Technology
& Computer User Groups**