

¹ Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[†] Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Why Teens Are at Risk for Identity Theft

Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook

Check your Facebook timeline. Chances are that with very little [Read story](#)



What is Caller ID Spoofing?

Your phone number plays a prominent role in identifying you [Read story](#)

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Vishing

Share this



Related articles

- SMSishing

SEE MORE ARTICLES

Vishing, (or voice phishing) happens when you receive a call on your home phone or mobile device, from someone pretending to be from a trusted source, like your bank. But is the voice on the other end really from your bank or is it just another identity thief fishing for your account information?

How Does Vishing Work?

When thieves go vishing, they'll call people using an automated system and leave messages saying there's a problem with your bank account or ATM card. The call will then direct you to a phone number or website that will ask for personal account information to verify your identity, but again, they're not verifying anything, they're stealing your account information. Then they're going to steal your money.

How Much Damage Can Vishing Cause?

According to an FBI scam alert, vishing victims reported having money illegally withdrawn from their accounts within 10 minutes of receiving the vishing call, and another of having "thousands of fraudulent withdrawals"¹ following a vishing call. If the transaction is done from a smartphone, it's also possible for thieves to gain access to all the information stored on the phone, as well.

Information thieves can collect:

- Personal information
- Account numbers and information
- PIN

What thieves can do with this information:

- Identity theft
- Bank fraud
- Other identity fraud

¹ www.fbi.gov/news/stories/2010/november/cyber.../cyber_11241

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[†] Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Why Teens Are at Risk for Identity Theft

Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook

Check your Facebook timeline. Chances are that with very little [Read story](#)



What is Caller ID Spoofing?

Your phone number plays a prominent role in identifying you [Read story](#)



Phone and Utilities Fraud Service agreements for cellular service or utilities are common means

[Read story](#)

Displaying 4 of 7 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001010

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



SMSishing

Share this



:



Related articles

- Smartphone Data Theft

SEE MORE ARTICLES

What is SMSishing?

Similar to phishing, SMSishing (or SMS phishing) is when a potential identity thief sends you a text message asking for personal or account information. Because the text appears to be from a reputable contact, many people respond, and that's when the theft begins.

Trick or Text?

The problem is obvious, once you have either called the telephone number provided or gone to the listed fraudulent website, you are asked to provide personal information – such as your bank account, debit card, PIN, or other numbers – to verify your identity. But nobody is verifying your identity. They're stealing it.

Information thieves can collect:

- Personal information
- Account numbers and information

What thieves can do with this information:

- Identity theft
- Employment-related fraud
- Loan fraud/payday loan fraud
- Bank fraud
- Benefits fraud
- Tax fraud
- Other identity fraud

FTC-0001011

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Why Teens Are at Risk for Identity Theft

Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook

Check your Facebook timeline. Chances are that with very little [Read story](#)



What is Caller ID Spoofing?

Your phone number plays a prominent role in identifying you [Read story](#)



Phone and Utilities Fraud Service agreements for cellular service or utilities are common means [Read story](#)

Displaying 4 of 7 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Card Skimming Scams on the Rise

By Marcia Simmons
June 25, 2014

Share this



Related articles

- NYC Restaurant Worker Accused of Identity Theft
- Skimming Devices

[SEE MORE ARTICLES](#)

When you swipe your card to buy gas or slide it into an ATM for cash, identity thieves may be able to gain access to your account number using a **card skimmer**. Once thieves have your card number, they can program it onto a dummy card and use it to tank your credit or drain your bank account.

The most common type of skimmer fits seamlessly over legitimate card slots a consumer would use, such as an ATM. Card readers that have been compromised usually look identical to their legitimate counterparts. Less-sophisticated handheld skimmers can be bought online for less than \$200. With these, a retail clerk or restaurant server can secretly swipe your card through their device after using it legitimately for your actual purchase. These are riskier for the thief, since they could be caught red-handed.

While this crime isn't new, incidents have been popping up more and more in the news recently.

A **card-skimming ring nabbed in Houston** was able to gain account data for 375 people from 35 skimming devices attached to drive-through ATMs. One man in the Chicago area is charged with skimming 200 debit card numbers from dozens of bank ATMs. A **California man was arrested for using a skimming device** on several pay-at-the-pump card slots.

Recently, a **Texas restaurant worker was caught on surveillance video** swiping customer cards on a handheld device. An **airport employee in Florida was charged with skimming** more than 100 customers' cards at the parking garage.

Experts recommend not using an ATM or other card reader, such as those at gas pumps or self-service grocery stores, if it doesn't look right to you. Sometimes the skimmers are so poorly installed that a quick tug will remove them. If that happens, alert the bank or store management and police. Since gas station pumps and ATMs are the most common targets, experts also suggest paying inside or withdrawing from inside the bank, as those machines are less vulnerable.

FTC-0001013

Some store employees are legitimately using handheld devices to get payments, such as the Apple Store or small businesses that deal primarily in cash but want to offer the convenience of card payments. To guard against handheld skimmers, experts say it's best to keep your card in sight whenever possible and to pay with cash if clerks or servers seem to be concealing their transactions.

Even the most vigilant consumers can find themselves victimized by card skimming. If you discover unusual transactions or other indications of skimming, contact your bank or credit card issuer immediately.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem

[Read story](#)

Ordering Free Credit Reports

Under U.S. law, you have a right to get your

[Read story](#)

Displaying 4 of 9 Results. [Show More Results](#)



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



What is a Credit Freeze?

By Beatrice Karnes
May 08, 2014

Share this



A credit freeze gives you the power to seize control of your financial information by preventing the release of your credit score and detailed reports by credit reporting agencies.

The three major U.S. credit bureaus—Equifax, Experian, TransUnion—earn their money by selling your credit information to other companies. Mortgage lenders, credit card companies, car dealerships and other agencies all purchase your information to decide if you are a good credit risk.

Lenders are unlikely to approve loans unless they know you're a good risk, so a credit freeze stops an identity thief from taking out mortgages or other debt in your name.

To place a credit freeze on your file, contact each credit reporting agency directly. Instructions are on the company websites:

- [Equifax](#)
- [Experian](#)
- [TransUnion](#)

If you have been a victim of identity theft it's free to place a credit freeze on your information. Consumers aged 65 or older often receive free credit freezes, or discounts. Otherwise, you may have to pay up to \$10 to each credit bureau to freeze your information. The cost is regulated by states, so the fee varies.

A credit freeze consists of three actions:

Related articles

- [ATMs Could be Vulnerable to Hackers](#)
- [New Account Fraud: The Cost of Remediation](#)
- [States Struggle to Make Birth and Death Certificat...](#)

[SEE MORE ARTICLES](#)

- Add - placing a freeze on your credit
- Lift - temporarily removing the freeze so you can apply for credit
- Remove - permanently removing the credit freeze

In addition to paying to add the freeze to your file, you may also be charged to lift your credit freeze. There is no cost for removal of the freeze.

There are downsides to weigh before deciding to place a credit freeze on your file. If you are planning to buy a home or car, rent an apartment, sign up for a cell phone plan or an account with a utility company, or apply for a credit card you will need to lift the freeze. Many employers also require credit checks of potential employees. If you pay a fee each time you request a lift of the credit freeze, the cost could quickly add up.

You may request a lift for a specific company, or for a set period of time.

Another consideration is that it takes 3-5 days to lift the freeze.

A credit freeze does not apply to current creditors. Also, government agencies such as the IRS may access your information in spite of a freeze.

One final note regarding your credit score: A credit freeze does not adversely affect it.

Beatrice Karnes is a freelance writer. She has many years of experience working behind the scenes at local TV stations in California, Colorado and Wyoming. Most recently, she was an editor for Patch Media, a local news and information consortium of 900 websites nationwide. Beatrice holds a bachelor's degree in journalism from San Jose State University.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is [Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide [Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem [Read story](#)

Ordering Free Credit Reports

Under U.S. law, you have a right to get your [Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

► Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Now is the Time to Plan for Retirement

By Jamie White
March 28, 2014

Share this



Are you planning for the future?

While retirement may seem like it's a long way off, saving for your later years "has to come first," stresses Liz Weston, a nationally syndicated personal finance columnist and author.

"You are so much better in the long run if you make this [saving for retirement] a top priority and keep your mitts off of it," Weston told LifeLock in an interview Friday.

People with retirement savings plans often get tax breaks, Weston said, allowing them to defer paying taxes on some of the money that's put into those plans.

An Individual Retirement Account, or IRA, lets people put away themselves for retirement. A 401(k) and similar accounts are known as workplace savings plans and are offered by employers. Employees decide whether to contribute a part of each paycheck before taxes are taken out.

Forty-four percent of all U.S. private businesses offer such plans, according to a March 2013 report by the U.S. Bureau of Labor Statistics. Some companies offer to match what an employee sets aside for a 401(k) account, usually up to a certain amount or percentage.

But even if your workplace doesn't have a matching program, you should still invest in a 401(k) if it's an option, Weston said.

"It is all the power of the future compounded: \$1,000 now is going to one day be \$10,000 and then \$30,000," she said, adding that she realizes it is harder for people in debt to realize the importance of saving for retirement and make it a priority.

About 51 million Americans have invested an estimated \$3.5 trillion in 401(k) plans, according to the Investment Company Institute. The organization says total U.S. retirement assets were \$23 trillion as of Dec. 31, 2013, up 5 percent from \$21.9 trillion on Sept. 30, 2013, and up 15.6 percent from year-end 2012.

Retirement savings accounted for 34 percent of all household financial assets in the United States at the end of the fourth quarter of 2013, according to the Institute.

Dan Solin, director of investor advocacy for the **BAM Alliance** and a wealth advisor with Buckingham Asset Management, offers ways to make the most out of your retirement savings plans in **an article published this week**.

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as

FTC-0001018

a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)

Ordering Free Credit Reports

Under U.S. law, you have a right to get your

[Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones

► Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

Ordering Free Credit Reports

Share this



Under U.S. law, you have a right to get your credit report for free once every 12 months from each of the three major credit bureaus -- Equifax, Experian and TransUnion -- and correct any mistakes you find on them. The credit reports include information on where you live, how much you owe on credit cards and loans, and how well you've met the agreed payment schedule for those cards and loans.

The three major bureaus have set up a centralized way to order reports from one, two or all three of them, and you can make the request online, by phone or in writing. Here's how to contact them:

- **Online:** <http://annualcreditreport.com>
- **Phone:** 1-877-322-8228
- **Mail:** Print out [this form](#), complete it, and mail it to the address on the form

Some people prefer to get an update once every four months by staggering their requests. If you request a free report from one bureau today, a second bureau in four months and the third bureau in eight months, you'll be getting more regular updates on your credit.

If you're a LifeLock Ultimate® member, this is one of the many things we handle for you. Just **log into your LifeLock account** to see your annual credit reports, along with annual credit scores and a monthly update of your TransUnion score.

Learn more about these free reports, along with what to do if you find errors on them, from the Federal Trade Commission's **Free Credit Reports** page.

More articles you might like:

CALL US AT
1-800-607-7205

Send us an email

Secure login



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

Now is the Time to Plan for Retirement

Are you planning for the



[Read story](#)

future? While retirement may seem [Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

► Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Are Debit Cards Dangerous?

By Jamie White
January 08, 2014

Share this



Related articles

- ATM Overlays
- Debit vs. Credit Card ID Theft

SEE MORE ARTICLES

January 7, 2014

For many people, debit cards have replaced checks or credit cards.

But in the wake of big news like the [theft of credit and debit card numbers from Target customers](#), some people are re-evaluating their use of debit cards.

Without the worry of accumulating a mountain of credit card debt, we swipe our debit cards and the money is immediately withdrawn from our bank accounts. No need to wait for a credit card bill to see how much we owe.

Because federal law limits responsibility for unauthorized credit card charges to \$50 and the four major credit card companies offer zero-liability policies, credit cards often provide better fraud protection than debit cards. [See what your bank says about liability for charges if your debit card was stolen in the Target breach.](#)

If someone gets a hold of your debit card, or even just the number and other pertinent card information, you are only on the hook for at most \$50 if you report the missing card or unauthorized transaction to your bank within two business days of discovering it.

But if you fail to report any fraudulent charges on your debit card within that two-day window, you could be liable for up to \$500. If you don't report unauthorized charges to your bank within 60 days of receiving your bank statement, all of the funds in your checking and/or savings accounts could be depleted. The Federal Trade Commission offers [detailed information on what the relevant laws require.](#)

Better Safe than Sorry

The four riskiest places to use your debit card, according to [Bankrate.com](#), are:

FTC-0001022

- ▶ Online to make purchases
- ▶ Gas stations
- ▶ Restaurants
- ▶ ATMs

'Credit' or 'Debit'

When you use your debit card, you're sometimes asked to choose "debit" or "credit." Some people think it's safer to pick "credit" over "debit." But choosing "credit" does not make it a credit card transaction, [reports CNBC contributor Herb Weisbaum](#).

What you are doing is choosing whether to enter a PIN or use your signature to withdraw that money out of your bank account.

While debit cards are convenient and not inherently dangerous, the bottom line is that credit cards offer better overall fraud protection. It can still be a good ideal to use a debit card when you want to limit your debt. Consider the debt-limiting protection of a debit card vs. the need to make sure you report any fraud quickly when deciding which card to use.

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem

[Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Other Types of Identity Theft

Share this



:



Related articles

- Types of Identity Theft

SEE MORE ARTICLES

Personal, criminal and insurance records are not things you typically think to monitor. But opportunistic thieves can exploit your good name for all it's worth.

How do other types of identity theft occur?

Identity thieves can use your personal information for a long list of crimes. They can subscribe to magazines, rent an apartment, obtain car insurance and a whole lot more. The crimes may seem small, but the effects can really add up. Anything tied to your personal information could be affected.

What are the effects of other types of identity theft?

Most cases of identity theft go unnoticed until you are notified by an outside source like a bank or credit union.¹ Until you catch the crime, identity thieves could be busy racking up debt and distorting your records. You could end up having to pay off large bills, and your credit could be negatively affected. With so many ways that an identity thief could use your information, the possible effects are endless.

The impact:

- Identity theft schemes classified as "other" make up 23% of identity theft complaints.²

¹ Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

² Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones
- Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Seniors at Risk for ID Theft

Share this    



Related articles

- Vishing

SEE MORE ARTICLES

Seniors are prime targets for identity theft.

Most seniors lead a different lifestyle than when they were younger. They have more free time and the children may have long ago moved out. Seniors have also spent their entire working life building a nest egg of retirement funds.

Identity thieves know this and they target seniors to take their identity and their finances. Their preferred method is the telephone. According to the National Crime Prevention Council, senior citizens are more at risk to be targeted by telemarketing scams than other age groups. These dishonest telemarketers direct anywhere from 56 to 80 percent of their calls to the elderly.

Why are senior citizens targeted so often?

Seniors are prime identity theft targets for a number of reasons. They often have saved a lot more money than younger people who are just starting out. At the same time, they have less people around to help them keep an eye on things.

Seniors are also more trusting of others and less likely to report identity theft because they don't want family members to think they cannot maintain their independence. An increased need for medical attention would mean increased use of Medicare, resulting in a lot of personal information at various medical facilities. Thieves may even target Social Security checks.

Identity protection tips for seniors.

If you're a senior and you want to help safeguard your identity yourself, there are numerous precautions

you can take. It's a lot of work but it could lower your risk.

- ▶ Keep personal information such as bank statements, Medicare statements and your Social Security number in a safe or safe deposit box.
- ▶ Don't carry your Social Security card.
- ▶ Keep credit card numbers secure, you'll need them if the cards are lost or stolen.
- ▶ If you pay bills by check, only include the last four digits of the account number.
- ▶ If you order new checks, pick them up at the bank rather than have them delivered.
- ▶ Opt out of direct mail offers at the FTC "OPTOUT" line (1-888-567-8688). These mailers include a lot of information and thieves can steal them from your trash.
- ▶ Never give out Medicare information over the phone or in answer to an email. Medicare will not request information this way. Better yet, never give out any personal information over the phone.
- ▶ If a caller claims to have a too-good-to-be-true deal, it probably is. Ask to see everything in writing before you commit.

If you suspect you've been a victim of identity theft, place a fraud alert at one of the credit bureaus: **Equifax**: 800-525-6285, **Experian**: 888-397-3742, or **TransUnion**: 800-680-7289.

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Youth at Risk

Share this



Related articles

- Campus Connection: Student ID Theft and Student Lo...

SEE MORE ARTICLES

Identity theft can be a nightmare at any age, but it can be even more devastating for young people who discover their good name and credit history were destroyed while they were still children.

Why Are Children Attractive Targets for Identity Predators?

Children make prime targets for identity thieves specifically because they have no credit history and thus, clean credit reports. Also, because parents don't think to check their children's credit histories, the theft can continue unchecked for over a decade. How appealing are children's identities to identity thieves? According to a recent news article, police agencies are saying children are now the fastest growing segment of identity theft victims.¹

How Do Identity Thieves Abuse Young Victims?

Identity thieves will use children's identities to take out loans and lines of credit they never intend to repay and to establish an identity so they can obtain things like jobs or a driver's license. The end result is that children can later be denied loans for cars or college, employment, a drivers' license, or the ability to obtain housing or utilities. How early does it start? Some parents have reported that their children began being victimized at as early as 11-months old.¹

Information thieves can collect:

- Social Security number
- Other personal information

What thieves can do with this information:

- Identity theft
- Employment-related fraud
- Loan fraud/payday loan fraud

FTC-0001030

- Bank fraud
- Benefits fraud
- Tax fraud
- Other identity fraud

¹ <http://www.businessweek.com/ap/financialnews/D9LNB7701.htm>

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[†] Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones
- Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

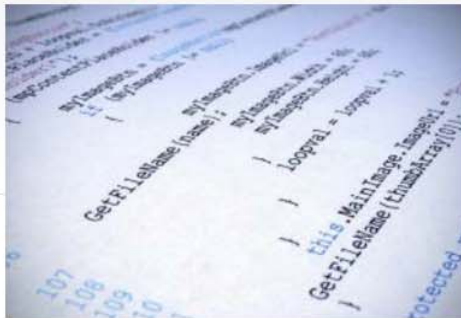
Send us an email 

Secure login 



Internet Privacy and ID Theft Protection

Share this



Related articles

- Counterfeit Website ID Theft

SEE MORE ARTICLES

Wherever you go online—they know.

You're being tracked online. The sites you visit, the products you purchase and even the location of your computer. It is often a harmless way for marketers to learn what products you like so they can better target their messaging. But sometimes it can pose a risk of identity theft.

Even if you're not snacking, you're leaving cookies all over.

Advertisers want to know who you are and what you do. They do this using an Internet or Browser "cookie." When you visit a website, you get a cookie—and it isn't chocolate chip. An Internet cookie is a unique ID that is part of your browser history. It stays with you as you jump from page to page within a site, and from site to site across the Internet. Over time, these cookies create a data cache that's extremely valuable to advertisers who are trying to learn your interests and habits.

So if you're online searching for information and great deals on winter clothing, advertisers will see a pattern in your cookie history and develop a profile. If they determine you're a good prospect, you'll suddenly see banner after banner trying to sell you everything from wool coats to a vacation in Maui.

Some view this as an invasion of privacy. Others see it as a great way get advertising that's relevant to their interests. But hackers see cookies as a way to piece together profiles for their attacks.

You're hunting for a great deal and being hunted at the same time.

Identity criminals use your cache of cookies to show them where to set their traps. Then they'll create sites that look a lot like the legitimate sites you frequent, with the sole purpose of asking you for personal information and stealing all they can—from your name to your Social Security number.

Protect yourself against identity thieves.

So what are your options? Deleting Internet cookies is a simple first step. Most online browsers have the ability to clear the cookie cache and browsing history. The challenge is remembering to do it on a regular

FTC-0001033

basis. And websites where you have a personal account will reload your unique cookie every time you visit.

Another option is to opt out of advertising. While all organizations give you the choice to opt out of their email advertising, not all let you opt out of their cookie tracking. Online businesses and advertising organizations are now using sites such as www.aboutads.info to give you the choice of opting out of cookie tracking.

Cookies can be effective for advertisers and convenient for customers. If you don't mind being targeted with messaging about the things you show interest in, at least be wary of emails or websites that appear to come from legitimate sources but request personal information.

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Debit vs. Credit Card ID Theft

Share this



:



Related articles

- [Protecting Your Plastic](#)

SEE MORE ARTICLES

Debit or credit?

Which type of card protects you the best? With over 1.5 billion credit cards and more than half a billion debit cards in use in the U.S.¹, millions of consumers have a choice, but some cards are safer than others.

Is it a stacked deck?

There are essentially four types of cards used to pay for goods and services—ATM, debit, credit and what are called virtual cards. ATM cards are used less often than in the past because they are cash withdraw cards only, although many people think of them as debit cards.

Debit cards are like an electronic check. You can access your bank accounts through ATM machines and make purchases paid directly out of your bank account. They have either the VISA or MasterCard logo, and they account for more than \$1 trillion in annual purchases made by U.S. consumers.¹

Credit cards are found in over 91 million American households.² They are not attached to bank accounts and payments can be made over time. You can also use them to withdraw cash at most ATM machines. Credit cards are issued by banks, retailers and other institutions, and those issued by VISA, Mastercard, Discover and American Express can be used at hundreds of thousands of locations around the world.

Virtual cards aren't physical cards at all. When you shop online, you can use an alternate number issued by your credit card company. It's often a temporary number for one time use and the transaction is billed on your regular credit card statement.

And the winner (loser) is...

Whether through physical theft, hacking, malware or data breaches, all individuals with any of these cards are subject to identity theft by having their card information stolen.

Carrying the least amount of risk is the virtual card, since it has a time or transaction limitation and there is

FTC-0001035

no personal information connected with it.

But in comparing the two most widely used forms of payment—debit and credit cards—credit cards offer more protection and less risk because funds are not being directly withdrawn from the user's bank account as it is with a debit card. Fraudulent withdrawals on a debit card can result in bounced checks and no access to cash while the bank investigates their report.

Additionally, most credit card companies allow 90 days for a victim to report an unauthorized transaction, while banks generally require a two-day notice for unauthorized debit card purchases. For debit cards, your loss is limited to \$50 only if you notify your financial institution two business days after learning of loss or theft. It then goes to \$500 until 60 days after the statement is mailed and becomes unlimited thereafter. For a credit card, your liability is limited to \$50 for any fraudulent use.³

Other steps for safer shopping.

First, make sure the website you're shopping on is secure and starts with an <https://> instead of <http://>. You'll also see a small lock on the lower right hand corner of the screen. This means the site is secure for transactions.

Don't do online shopping in public places such as coffee shops or public Wi-Fi areas. Their networks are usually unsecure and the information you are entering might be stolen right there at that location. Finally, avoid using retail websites to store your personal and payment information. Although it speeds up the checkout process, it leaves your identity and financial information exposed should that server experience a data breach.

¹ Creditcards.com, Credit Card Statistics, Industry Facts, Debt Statistics,

² ITRC Face Sheet 131 – Credit Card vs. Debit Card,

³ FTC Fair Credit Billing Act

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

► Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Identity Theft Victim? Start Here

By Genevieve Bookwalter

July 28, 2014

Share this



You just realized you are a victim of identity theft. Now you're not sure where to start in notifying credit agencies, banks, credit card companies and more. Check out our list below of links to letters from the [Federal Trade Commission](#) that will help get you started. They did the wording. You fill in the details.

— Do you need to dispute charges that you didn't make to your cards or accounts? [This sample letter](#) will help you get the word out to banks, credit card companies and others.

— If your credit report shows a fraudulent new account opened in your name, [this sample letter](#) will help you report the account to the company and close it.

— If you spot errors on your credit report, [this letter](#) will help you ask credit reporting companies to remove the problems.

— [This letter](#) will help you ask businesses to stop reporting fraudulent information on existing, legitimate accounts — like charges you didn't make — to credit reporting companies.

— [This letter](#) will help you ask businesses to stop reporting new accounts that were fraudulently opened in your name to credit reporting companies.

— If businesses have already reported fraudulent information to credit reporting companies, use [this letter](#) to ask those companies to remove it.

— Curious about the documents a thief used to steal your identity? Use [this letter](#) to ask for copies.

— If debt collectors are hassling you to pay for charges in your name that you didn't make, [this letter](#) will help you ask them to stop.

Related articles

- [Card Skimming Scams on the Rise](#)
- [Identity Theft vs. Credit Card Fraud](#)
- [Identity Thieves Target Medical Records](#)

[SEE MORE ARTICLES](#)

FTC-0001038

Most of these letters require you to include a copy of your identity theft report. Some also ask that you include your credit report and a copy of the account statement showing the items in dispute.

Good luck!

Genevieve Bookwalter is a freelance journalist based in the San Francisco Bay Area. She has worked as a writer, reporter and editor for more than a decade. Her work has appeared in The Los Angeles Times, WIRED, San Jose Mercury News and other newspapers nationwide. She is a graduate of the Science Communication program at University of California Santa Cruz, and holds bachelor's degrees in art and science from the University of Illinois at Urbana-Champaign.

More articles you might like:



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



P.F. Chang's Continues to Grapple with Breac...

P.F. Chang's China Bistro learned of a security breach involving [Read story](#)



Police: Man Rents Lavish Car, Home on Stolen Credi...

A 19-year-old from Rohnert Park, Calif., has been arrested for using [Read story](#)

[Read story](#)

Displaying 4 of 7 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Identity Thieves Come in all Shapes and Sizes

By Marcia Simmons
June 04, 2014

Share this



Whether they're targeting Army records, housing applications, brokerage accounts or even your own mailbox, identity thieves of all stripes are in the news for victimizing innocent people.

Soldier Faces Decades in Prison for Identity Theft

An active duty officer pleaded guilty to stealing the identity of other soldiers and applying for loans in their names, [according to the Army Times](#).

James Robert Jones, who worked with the U.S. Army Office of Inspector General at Fort Campbell in Tennessee, admitted to using his position to get personal identifying information of active duty U.S. Army officers, including officers who were deployed to Afghanistan.

Authorities say that Jones asked a colleague to delete records from his Army laptop and tried to blame the activity on a dead officer who was never involved in the scheme.

Jones faces up to 30 years in prison for the bank fraud charges, up to 20 years in prison for obstruction of justice, and up to 5 years in prison for making false statements. Jones will be sentenced on Aug. 11.

Virginia Man Sentenced for Stealing IDs from Housing Applications

Donte L. Battin was sentenced to 6-and-a-half years in prison for his role in an \$87,000 identity theft scheme that victimized housing applicants, [the Washington Times](#) reports.

Along with four accomplices, Battin stole personal information from people who applied for housing at North Shore Garden Apartments in Virginia. Authorities say the team then used the information to empty victim accounts at a credit union and apply for loans in their names.

Battin pleaded guilty to bank fraud charges and aggravated identity theft.

Man who Posed as Fidelity Broker Pleads Guilty

A Massachusetts man has pleaded guilty to convincing elderly people he worked for Fidelity investments and then stealing money from them, [the Boston Business Journal](#) reports.

John Michael Babiarz was fired from New York brokerage firm Bishop, Rosen & Co. then told some of his clients he moved to a job at Fidelity and could continue to manage their money. Authorities say he then obtained their private information and passwords under the guise of setting up new accounts.

Babiarz had been previously charged in an administrative complaint by the state securities division.

When sentenced in August, Babiarz faces 20 years in prison and fines up to \$500,000.

FTC-0001040

Oregon ID Thief Gets 3-year Prison Term

Michelle Renee Lustig was sentenced to 3-and-a-half years in prison for stealing mail and using it to commit identity theft, [the Mail Tribune reports](#).

Lustig was also ordered to pay \$12,387 in restitution. Her accomplice, Gregory Stephen Brooks, was sentenced in April to nearly seven years for his role in their four-month identity theft scam.

The two used information stolen from mailboxes to open credit card accounts in victims' names and engage in fraudulent banking activities. Lustig also printed counterfeit checks in the victims' names.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



The Trouble With Tax Returns

Share this



:



Related articles

- Tax Fraud

SEE MORE ARTICLES

The side effects are nothing new. Tax season: may cause anxiety, nausea and depression. But an accurate return is only half the battle. The latest gripe? Identity theft tax fraud. Go ahead and add it to your list of tax season woes.

From 2009 to 2011, the IRS estimates that 404,000 people were victims of identity theft tax fraud. And it's only getting worse. The IRS saw **a huge increase in this type of crime** from 2010 to 2011.

Think about what's on your tax return: personal information, employment history, loan details, banking data, birthdates and that coveted Social Security number.

That's a lot of information on one document. In fact, it's a PPI gold mine. What's PPI? It's your protected personal information. And it's hidden treasure to identity thieves.

The goods news is the IRS has improved its ability to detect tax fraud, stopping nearly \$1.5 billion in fraudulent refunds. The bad news? With over 100 million tax refunds to process each year, the IRS can't catch everything.

And that's only half of the problem—it doesn't stop at tax fraud. With that much information, an identity thief could commit a long list of crimes.

As we apprehensively near that looming April deadline, try not to get too overwhelmed or stressed. Instead, take some time for a few extra precautionary steps. The safety of your information is just as important as getting your taxes done.

Here's five tips to secure your PPI during tax time:

1. Secure your connection

If you e-file, do not login on public Wi-Fi. Instead ensure you're on a private, protected Internet connection. Also be sure that you are on a secure website (look for the "https:" in your browser's address bar) and on a computer with a working anti-virus system.

2. Don't get phished

The IRS will never contact you through email, so do not respond if you receive any emails claiming to be from the IRS. They could be fraudsters trying to trick you into providing personal information. Learn more about protecting yourself against phishing attacks [here](#).

3. Lock up your returns

What's worse than getting robbed? Getting robbed AND getting your identity stolen. Keep all of your tax information and returns in a locked safe. And don't keep old tax information stored on your computer. It should all be in that locked safe—print out a hard copy or move it onto an external hard drive.

4. Stay off of file-sharing programs

Many people use file-sharing programs to download music or movies. These types of websites put users at a serious risk of being hacked, often times without being detected. Once they've hacked your computer, identity thieves could steal tax information right off of your hard drive.

5. Trust the experts

Make sure that your tax professional is licensed, affiliated with a professional organization or listed with the Better Business Bureau, the state board of accountancy or another trusted institution.

Source: "IRS Faces Surge in Identity Theft Tax Fraud." [www.lifeinc.today.msnbc.msn.com](http://lifeinc.today.msnbc.msn.com).

http://lifeinc.today.msnbc.msn.com/_news/2012/02/17/10428874-irs-faces-surge-in-identity-theft-tax-fraud?chromedomain=usnews. February 17th 2012.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205



New Account Fraud: The Cost of Remediation

Share this



Related articles

- Tax Fraud

SEE MORE ARTICLES

Congratulations, You've Been Approved

There's a major difference in receiving a pre-approved credit card in the mail and receiving an actual credit card in the mail. The former implies a creditor wants your business. You can shred the card, remove yourself from the pre-approved credit card mailing list and get on with your life.

But receiving an actual, approved credit card in the mail is not the same thing. In fact, this could mean that an identity thief has opened credit in your name. By the time that card lands in your mailbox, it may already be maxed out and accumulating interest. Merely cutting up the card and throwing it away isn't going to fix the problem.

In the event that you do receive a credit card in the mail—say from a credit union or popular retailer—it's important to quickly jump into action. Similar to any identity theft resolution process, the steps to clean your name can cost you a lot of time and a lot of cash.

The Most Expensive Type of Fraud

When it comes to identity theft, the resolution path can be tedious and expensive no matter what type of fraud has occurred. But new account fraud—including new credit cards—is the most expensive type of identity fraud for victims to resolve.¹



In a 2011 study done by Javelin Strategy & Research, victims were asked to provide a few details regarding the cost of resolution in their identity theft experiences. Here's what the numbers show.¹

Average resolution time for victims of all types of identity theft: **12 hours**

Average consumer cost of identity theft resolution: **\$354**

Average resolution time in new account fraud: **26 hours**

Average consumer cost of identity theft resolution in new account fraud: **\$1,205**

The Recovery Expense Report

The victims surveyed were not given specific examples of common resolution costs or tasks, but there are several steps to resolution that are crucial—no matter what the expense. Here are a few of these steps:

(These numbers are an approximate representation. Actual costs will vary.)

Step 1: Contact the retailer where the fraudulent account was opened

If you receive a fraudulent credit card in the mail, immediately call the fraud department number on the back of the card. Have your information ready. In most cases, you will be asked to verify that the account is linked to your name and Social Security number.

After you have verified that the card is indeed fraudulent, you must specifically ask the company to start a fraud investigation. This often requires some paperwork. To speed up the process as much as possible, comply with the creditors requirements and requests.

It's also important to specifically insist that the company removes the credit application from your credit report. This type of transaction affects your credit score, so this step is critical.

Once the company has all the information they need, they will give you a fraud investigation case number. Be sure to keep this number, and any other related information, in a safe place.

Possible Costs:

- Printing costs: 4 pages for \$.25²
- Certified mail: \$.10³
- Lost 5 hours of work: \$36.25⁴

Possible Time:

- 1-3 hours on the phone
- 60 minutes of paperwork

Step 2: File a police report with your local police department

Next, head to your local police department. You must file a report with the department located in the city where you lived when the fraud occurred.

Unfortunately, identity theft is still a widely unknown crime. Be prepared to be persistence and do some studying before you go. The *Identity Theft and Assumption Deterrence Act* states that as an identity theft victim, you have a right to file a police report. In many cases, there is a police report fee.

Possible Costs:

- Gas Money: \$2.04⁵
- Lost hour of work: \$10.86⁴
- Police report fee: \$7.58⁶

Possible Time:

- Driving: 30 minutes
- Filing report: 60 minutes

Step 3: Make an FTC complaint

Head to FTC.gov and fill out the **complaint form**. The complaint form will also serve as an Affidavit form. Keep a copy of the Affidavit in a secure place.

Possible Costs:

- Print Affidavit: 7 cents²

Possible Time:

- 15 minutes

Step 4: Put a seven-year alert on your credit reports

In order to set a seven-year credit freeze, you will need to contact each of the three credit bureaus separately and mail them the requested information. These requests usually include a copy of your Social Security number, Driver's license and proof of residence.

You will also need to send a copy of your police report and/or your Affidavit, plus any other information that the credit bureaus request. We recommend sending these confidential documents over certified mail rather than standard so that you have proof of delivery. With so much private information in one envelope, the more safety precautions you take, the better. **FTC-0001047**

Possible Costs:

- 3 packets certified mail: \$24.30³
- Copies- 31 pages: \$2.00²

Possible Time:

- 60 minutes on phone
- 60 minutes for 3 packets

Step 5: Order credit reports

You will want to verify that there is no other fraudulent information on your credit reports, so you will need to request a credit report separately from each of the three bureaus. If this is the first time you are requesting reports within a year, then the service will be free. You can request your free credit reports by heading to AnnualCreditReport.com. Otherwise, you will have to pay full price.

Possible Costs:

- \$40* to order 3 from Experian⁷

Possible Time:

- 15 minutes to order
- 30 minutes to review each

Step 6: Request credit reports again, 90 days after resolution

Once the investigation is over, you should receive a letter from the card issuer stating that the crime has been resolved and your identity has been removed from the debt. Ninety days after you receive this letter, you should request your credit reports again to ensure that this information has actually been removed from your credit reports.

Possible Costs:

- \$40* to order 3 from Experian⁷

Possible Time:

- 15 minutes to order
- 30 minutes to review each

By the end of this hypothetical situation, your total cost is **\$171.63** and the total time spent to resolve the issue is **9.25** hours. But if an identity thief was able to open one account, it's likely the crook may have opened another—meaning you're repeating many of these steps all over again. And these numbers only reflect some common expenses at national averages.

The Fine Print

Identity theft is a complex crime, and a victim's busy lifestyle only adds more obstacles. That means there's a long list of potential expenses and time-consuming tasks involved in resolving the crime. When considering an identity theft protection service, try to remember all the small costs and tasks that might add up if you don't have protection, such as:

- Time off work
- Babysitters
- Time spent on the phone
- Mail expenses
- Driving time (post office, police department, etc.)
- Gas money
- Faxing, scanning and/or copying
- Additional fraudulent accounts
- Complications due to credit deadlines and legality
- Delays due to holiday hours and scheduling

The Right Protection Offers Remediation

An identity theft alert system is a great feature for peace of mind. It can help consumers stay ahead of an identity thief. But what happens after the alert? What happens if an identity thief does cause damage to a member's identity?

Most identity theft services offer both an alert system and remediation services. And those remediation services may cover some or all of the above expenses, as well as facilitate the process.

Before you buy, be sure to ask what happens if you do become a victim. Comprehensive protection should come with comprehensive remediation.

For more information about recovery steps, [click here](#).

* Consumers can order free credit reports once a year

¹ "2012 Identity Fraud Survey Report." Javelin Strategy & Research. February 2012.

² Average 6.37 cents a page. Dover-Sherborn Technology. hs.doversherborn.org. **FTC-0001049**/19/2012.

<http://hs.doversherborn.org/technology/printing.htm>.

3 "Postal Price Calculator." United States Postal Service. Standard Priority envelope from LifeLock to Best Buy headquarters in Minneapolis.

4 National average for minimum wage: \$7.25. "Wage, and Hour Division." United States Department of Labor. Accessed 11/19/12. http://www.dol.gov/whd/minimumwage.htm#UKVr5eOe_rg

5 Based off of the "Fuel Calculator" at <http://www.city-data.com/gas/gas.php>. Chevy Malibu is most popular car in US: <http://www.nytimes.com/interactive/2012/09/16/automobiles/contenters-for-americas-most-popular-car-the-latest-wave-of-midsized-family-sedans.html>. National gas price average is \$3.416. <http://fuelgaugereport.aaa.com/?redirectto=http://fuelgaugereport.opisnet.com/index.asp>

6 Hartley, Eric. "Fees for court and police records vary—and L.A. city and county agencies charge far more than most." 07/2/2012. Daily News Los Angeles. Accessed 11/19/2012. http://www.dailynews.com/news/ci_21180313

7 3-Bureau Credit Report and Score. www.experian.com. Accessed 11/19/12.

Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach
[Read story](#)



Russian Crime Ring Steals Billions of Passwords, O...
A Russian Crime ring has gathered what may be the
[Read story](#)



What To Do If Your School or Your Child's Sc...
A data breach reported at Butler University in Indianapolis in June exposed
[Read story](#)



Tax Forms from Another State Pose Problem
If you received a letter saying your tax return is
[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

FTC-0001050



Copyright © 2006-2014. Lifelock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Identity Thieves Target Medical Records

By Marcia Simmons
June 17, 2014

Share this



Medical records contain personal information that can give thieves everything they need to steal your identity. Whether through fraud or carelessness, the very employees trusted to protect these records are the ones often putting you at risk. Here are several cases showing just how vulnerable medical records can be.

Related articles

- Identity Theft Hits Thousands of Medical Patients
- Medical Records Hot Commodity for Identity Thieves
- School Data Breaches Leave Young Children Vulnerab...

SEE MORE ARTICLES

Woman Gets 16 Years for Scamming Medicaid With Kids' Stolen IDs

A Georgia dietician was sentenced to 16 years in prison for stealing the identities of Head Start students to claim more than \$4 million from Georgia Medicaid, according to [The Florida Times-Union](#).

Schella Hope claimed at trial that other people forged her signature to involve her company, Hope Nutritional Services LLC, in the fraud. A federal jury convicted hope of 58 counts, including conspiracy to commit health care fraud, aggravated identity theft and money laundering.

Officials say Hope stole the identities of 25,000 children across Georgia and invented medical conditions to add to their files in order to bill government programs for services.

The judge ordered Hope to repay more than \$4 million and sentenced her to three years' probation upon release.

Health Department Clerk Steals Over 1,500 Patient IDs

A former health department employee was sentenced to two years in prison for stealing patient information, [CBS Miami reports](#).

Authorities say Salita St. Simon stole the private data of 1,858 people when she was a senior clerk in the
FTC-0001052

Palm Beach County Health Department. She then passed it on to others who used it to file fraudulent tax returns.

The judge also ordered St. Simon to pay more than \$19,000 in restitution and serve two years' probation after her release.

VA Accidentally Releases Thousands of Medical Records to 1 Patient

When a veteran ordered his own medical records from a Veterans Affairs Medical Campus in Wyoming, the VA sent him a CD containing over 6,000 pages of private medical information for other patients, [FOX31 Denver reports](#).

While the man who received the records wishes to remain anonymous, FOX31 contacted one of the men whose medical information was on the CD.

Terry Teg was unaware his medical records had been sent to a stranger until he was contacted, but he wasn't surprised. The Cheyenne VA facility had mistakenly sent him someone else's medical records in the past.

A VA spokesperson says an employee realized the mistake after the records were mailed.

In the last three months of 2013, the entire VA system experienced about 2,300 record breaches and offered those veterans credit protection.

Pennsylvania Health Center Mixes Up Patient Records

Coordinated Health in Pennsylvania sent one patient home with another patient's records, according to the [Standard Speaker](#).

Gloria Senape was sent home with the private information of another patient, but later told that her information was not given to anyone else. The company will now provide credit monitoring and protection services for her.

Earlier this year, Coordinated Health had larger security issues when an employee laptop containing 733 patient records was stolen from a car.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

FTC-0001053

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones

▸ Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

Send us an email 

Secure login 



More Than Just a Lost Wallet

Share this



Related articles

- Mail Theft

SEE MORE ARTICLES

By now, most of us know that leaving a Social Security card in a purse or wallet is a recipe for disaster. But what about standard wallet items? A lost wallet is much more than an inconvenience or lost cash.

A friend of mine lost his wallet during his final year at college. Like most students eating lunch at the student union, his packed schedule offered him only a short break for lunch. He was in such a hurry that he didn't realize his wallet fell out of his pocket after he paid for his meal. No big deal, he thought. He doesn't carry much cash, and he can cancel his credit and debit card. Unfortunately, a wallet in the wrong hands gives enough personal information to wreak havoc.

Once upon a time, it was commonplace for colleges and universities to use Social Security numbers on their student identification cards. They probably figured students already have a unique identifier, why bother creating a new string of numbers for each student? Well, that was the case at my friend's university. His campus ID featured his full name and Social Security number (SSN). His driver's license featured his current address. You can already see where this story is heading.

The wallet was picked up by a fellow student. Rather than contacting my friend or the university, this student decided to use the found item for profit. This is how normal people become identity thieves. Identity theft is a crime of opportunity, and thanks to lax policies there are plenty of opportunities.

It took my friend several months to discover his identity was compromised. He graduated and was applying for a car loan. He was denied because of an extremely low credit score. This took him by complete surprise because he never missed a credit card payment in his life. He thought he had established stellar credit. Well, he had. Unfortunately that identity thief used that stellar credit to rack up credit cards that were never paid off.

The sad thing is this story could have ended with just a lost wallet if only more organizations had better security practices. Thankfully most colleges and universities no longer use SSNs on college IDs. Many states now forbid public schools from using the SSN in lieu of a different number. That doesn't mean that

FTC-0001055

security practices are perfect. Some campus bookstores require students to write their SSN on personal checks. In several instances, professors posted grades sorted by student SSN! Unfortunately we cannot control how institutions use our personal information. But we can establish best practices for personal information security, which we will share on this blog regularly. Also remember you are entitled to **free annual credit reports**, so you can monitor for suspicious activity before applying for that car or mortgage.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



The Dangers of Medical Identity Theft

By Marcia Simmons
June 23, 2014

Share this



Related articles

- Identity Thieves Target Medical Records
- School Data Breaches Leave Young Children Vulnerab...

[SEE MORE ARTICLES](#)

While we all know our bank accounts and credit are at risk, there's another type of identity fraud that is on the rise. Medical identity theft accounted for **43% of all identity theft reported in 2013**.

Between 27.8 and 67.7 million people's medical records have been breached since 2009, according to the U.S. Department of Health and Human Services estimates.

There are **cases of opportunists** who **use identities of someone they know** to get treatment. Some thieves hack medical provider records, while others are health care employees who use their access to sensitive data for personal gain. However they get your information, once they have it they can get medical treatment or prescriptions in your name.

About 36 percent of medical identity theft victims in 2013 paid an average of \$18,660 because of the fraud, according to research by the Ponemon Institute. But the damage from this type of theft can be more than financial.

By contaminating your medical records with their information, a thief turns them into an inaccurate and potentially dangerous false documentation of important facts such as your blood type, allergies, past medical procedures and more. Fixing this information is time-consuming. But if you don't know it's inaccurate to begin with, it could endanger your health in an emergency.

If your insurance company thinks you've already used your coverage for certain treatments, you may not be covered once you need to use your insurance due to yearly care caps, limits on certain prescriptions or procedures that can only be covered once in a lifetime, such as a heart transplant.

Ponemon research also found that many health care organizations allow employees to use their own personal mobile devices and computers to connect to sensitive records. Very few required their employees to install anti-virus or anti-malware software.

FTC-0001057

To protect yourself, be sure to ask your insurers for a list of benefits paid out to you at least once a year to ensure it's correct. Read every notice you get in the mail with an eye for any treatments or prescriptions that aren't familiar. It's also wise to take as much care with your health insurance card and medical information as you would with your credit cards and financial information.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



to grab card information from 20 customers.

The woman cooperated with police when caught and authorities were able to find Liggins because a photo on Instagram of his high school diploma showed his full name. Police monitored a meeting between her and Liggins to exchange card machines and later arrested him.

Authorities found skimmers, stolen identities and computers used for the fraud at his home.

Man Arrested for ID Theft for Impersonating TV Weather Man Online

Matthew Wendt was arrested for impersonating a TV meteorologist on social media to meet women, [KWQC reports](#).

TV personality Greg Dutra discovered the fraud when he tagged his girlfriend in a Twitter post and another woman contacted him, upset because she'd been romantically involved with him on Facebook. Only it was actually Wendt who had been contacting her on Facebook pretending to be Dutra.

Police tracked Wendt through his IP address and are investigating what personal information of Dutra's he has and whether he obtained personal information from the women he contacted.

Wisconsin ID Thief Identified Through Police Facebook Page

Racine police nabbed a suspected identity thief using Facebook, [according to the Journal Times](#).

Authorities say Shane R. Trentadue was filmed by an ATM camera using a stolen debit card. Police received tips from the public about his identity after putting snapshots from that footage on Facebook.

Trentadue was charged with fraudulent use of a credit card and felony identity theft.

Authorities Warn Fake Instagram Account Could Lead to ID Theft

A fake Instagram account created in the name of lottery winner Solomon Jackson Jr. could open many people up to identity theft, [WACH reports](#).

The bogus posts claim Solomon will give a \$1,000 scholarship to the first 100,000 followers of the account.

Authorities say scammers know what kinds of social media stunts are trending and use schemes like this to collect personal information from unsuspecting people looking to win a few bucks.

Fellow Instagram users caught on to the scam, as have authorities, and are warning others not to give any personal information to this or similar users.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Back to School: How College Students Can Protect t...

So you, or your freshly-minted university student, are headed off

[Read story](#)



Back to School: How to Keep Your Child's Ide...

With Back-to-School time rapidly approaching, parents are soon to be

[Read story](#)



Why Teens Are at Risk for Identity Theft

Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook

Check your Facebook timeline. Chances are that with very little [Read story](#)

Displaying 4 of 5 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

▸ Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



5 Ways to Prevent Identity Theft While on Vacation

By Beatrice Karnes
June 11, 2014

Share this



A summer vacation is a wonderful way to shed stress, explore new places and cultures, and reconnect with the people who mean the most to us.

Unfortunately, we all know that a vacation can be ruined by criminals. Taking a few precautions, beginning when you're still at home, could make the difference between happy memories and a long-term nightmare. These five simple steps could prevent identity theft:

- 1. Clean out your wallet** — You've been meaning to do this anyway. Shred all receipts or file them at home. Put your checkbook in a safe place in your home, and use your credit or debit card while traveling, or traveler's checks. Leave gift cards at home unless you plan to use them on vacation. You should never routinely carry your Social Security or Medicare cards. If these are in your wallet, remove them permanently.
- 2. Notify your credit card provider** — Once you've decided which credit or debit card to take on vacation, contact the company to let them know where you'll be traveling and for how long. Likewise, contact the providers of cards that you're leaving behind. The fraud units of all cards will know where you are to prevent unauthorized purchases.
- 3. Take a spare wallet** — Tuck a little bit of cash inside along with a hotel keycard from a previous trip. Men should carry this in their rear pants pocket while women should carry this at the top of items in their purse. If you're the victim of a pickpocket, this wallet will be stolen, not your real one. If a robber asks for your wallet, hand over the spare.
- 4. Don't post vacation photos on social media** — Posting status updates that you're away from home

Related articles

- Beware of Fraud When Looking for Love Through Onli...
- Credit Card RFID Chips Magnets for Identity Thieve...
- What to do When You Lose Your Wallet

[SEE MORE ARTICLES](#)

and fun vacation photos may seem like a good idea, but really any of this personal information is useful both to burglars and identity thieves.

5. Phone calls from “front desk fraudsters” — If you receive a call from the “front desk” saying there’s a problem with your credit card and they need a number from a different card, politely tell them that you’ll call back in a moment and hang up. Call the desk yourself to check if the call is legitimate. You may find out that an identity thief was trying to steal your card number or, if there is a genuine problem with your card, call the company to fix the problem.

Beatrice Karnes is a freelance writer. She has many years of experience working behind the scenes at local TV stations in California, Colorado and Wyoming. Most recently, she was an editor for Patch Media, a local news and information consortium of 900 websites nationwide. Beatrice holds a bachelor’s degree in journalism from San Jose State University.

More articles you might like:



Back to School: How College Students Can Protect t...
So you, or your freshly-minted university student, are headed off

[Read story](#)



Back to School: How to Keep Your Child’s Ide...
With Back-to-School time rapidly approaching, parents are soon to be

[Read story](#)



Why Teens Are at Risk for Identity Theft
Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook
Check your Facebook timeline. Chances are that with very little [Read story](#)

Displaying 4 of 6 Results. [Show More Results](#) ▶



Relentlessly Protecting Your Identity

Call Us 1-800-607-7205

Login

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

▶ **Understanding Identity Theft**

Electronic Communication

Fraud

Social Networks

Fish Out of Water

Share this

Twitter

Facebook


Google+

LinkedIn

Related articles

- **Danger of Malware**

SEE MORE ARTICLES



An Introduction to the Newest Trend in Identity Theft

Let's try to have some compassion; identity thieves are people, too. True, they're often looking to steal your money, use your health insurance, gain employment or start a new small business with your name and SSN. But sometimes, they're just looking to fall in love.

At least that's the basis of the term "catfish"—made popular by the recent Manti Te'o scandal, but first hitting the media in the [2010 documentary](#) aptly titled, *Catfish*.

Catfish, Kind of Like Catphish
(Spoiler Alert)

The plot of *Catfish* seems simple: A couple falls in love online and spends countless hours talking on the phone. But as the lies unravel, things get complicated. By creating a fake Facebook profile and network of friends, the woman has tricked our protagonist into falling in love with a façade.

The film ends unexpectedly with the woman's *husband* recounting a tall tale about the sea-dwelling catfish's role in the transportation of cod from Alaska to China. In this ironic moment, the husband draws a metaphorical explanation of his wife's odd and manipulative behavior as a catfish. **FTC-0001064**

CALL US AT
1-800-607-7205



And thus the term "catfish" was born.

Catfish: – noun /Kat – Fi – SH/

A person who steals someone's social media identity to create a fake persona—complete with a fully-functioning Facebook profile and a masterful masquerade of family members, friends and coworkers—with the end goal of seducing a partner into a long-term online relationship.

Sadly, every catfish has a catfisher—the person that fell in love with the façade.

The **MTV show** of the same name features a new love/rom protagonist every week who is seeking to meet his/her long-distance lover. Almost every episode ends with a catfish exposed. As the season continues it becomes clear: there seems to be a lot of catfish out there.

Another Way to Say "Identity Thief"

Although the footage is entertaining, the facts are alarming. A catfish is just another kind of identity thief, and these thieves can steal personal information and photos from multiple victims to not only create a *fake* Facebook profile, but also a *fake* Facebook network of *fake* friends with *fake* profiles consisting of more stolen (*i.e. fake*) photos.

True, merely tricking someone into falling in love, although emotionally tolling, is relatively harmless. But what if an identity thief uses the fake profile to gain employment or scam people into giving money or more information? The consequences could be devastating.

As the term and trend gain popularity, it's likely that catfishing may become a more common form of identity theft. So it's smart to take some proactive steps. This unique crime requires that you protect yourself from both being catfished and having your identity stolen for the use of a catfish.

There Are Other Fish in the Sea

Tips to Avoid Being Catfished:

1. Use your webcam

If you meet someone online, take advantage of video chat at the beginning of your interactions.

There are several free options including Skype and Google Plus. If computer technology is a problem, set up a time where you can both be at a library or Kinkos with web camera capabilities. If your significant other makes excuses, you should consider this a red flag.

2. Save it for the first date

Although things might seem intimate at first, be weary of getting too close too fast. Until you meet your new love interest in person, do not give out any personal information that could be used for identity theft.

3. Do your research

There are plenty of ways to find out more information about your cyber sweetheart. Start by doing a simple online search of his/her name and city. There are also sites that offer free background checks.

If you can't dig up any information, research the validity of some of your partner's closest social media friends. Consider even reaching out to those friends directly to get a reference.

Tips to Avoid Becoming a Catfish Resource Center:

1. Set up a Google alert for your name
An easy, proactive way to ensure your social media profiles aren't being duplicated is to set up a Google Alert for your name. If someone creates a fully functioning profile with your name, you will get an alert.
2. Reverse photo search
Set up a calendar or phone alert to remind yourself to do periodic reverse photo searches. Just drag your profile photo into the search bar, and Google will search for matches to this photo. This is a great way to find out if someone is using your profile picture for his/her own account.
3. Photo Privacy settings
Make sure all of your photos online are set to private. That includes Facebook, Google Plus and Twitter. Many photo storage sites like Flickr can be easily viewed by the public if not set up properly so check the settings on those accounts, too.

As always, caution is key when it comes to security.

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.
 † Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



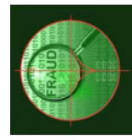
Tips to Avoid Medicare Card Fraud
Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...
As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation
A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



How to Pick a Secure Password

By Jamie White
November 21, 2013

Share this



Related articles

- How to Protect Your Identity
- Protecting Your Password

SEE MORE ARTICLES

In the movies, hackers make it look easy to crack a password. The fact is, it often is as simple as it seems on the big screen. "While passwords are a vital component of system security, they can be cracked or broken relatively easily," according to software company Symantec.

And once thieves break into your accounts, your personal information and identity are at risk.

But there are simple steps you can take to choose a secure password.

1. Be unconventional.

Avoid common words anyone can find in the dictionary, and simply adding numbers to common terms, like mainstreet12, isn't any better. Hackers write programs to crack these types of passwords first.

2. Stay impersonal.

Many people use birthdays, addresses or other personal info to make passwords memorable. But it is "alarmingly easy" for hackers to obtain personal information about prospective targets, according to Symantec. Avoid anything that refers to your name, nickname, the name of a family member or pet and any personal numbers like phone numbers, addresses or other information.

3. Be complex.

The longer and more complicated your password is, the harder it is to guess. Include numbers, symbols and mixed-case letters. **Google suggests this technique:** Create a phrase known only to you, and associate it with a particular website. A phrase for your email could be "My friends Tom and Jasmine send me a funny email once a day." Use numbers and letters to recreate it. "MfT&Jsmafe1ad" is a password with lots of

FTC-0001068

variations," notes Google.

4. Mix and match.

Do the same to create a unique password for every other password-protected site you visit, Google suggests.

"Choosing the same password for each of your online accounts is like using the same key to lock your home, car and office—if a criminal gains access to one, all of them are compromised," it says.

5. Change them up.

Passwords should be changed regularly to remain effective. How often?

Online financial accounts should be changed every month or two; corporate network passwords every 3-4 months. Everything else? Simply use good judgment and don't be lazy.

"Changing a password is relatively quick and painless compared to the irritating and expensive process of combating identity theft."

6. Put it to the test.

Online password checkers can evaluate a password's strength. Microsoft has a [password checker here](#).

7. Consider a password manager.

[Connectsafely.org](#) suggests using a program or service like [RoboForm](#), [LastPass](#) or [Password Safe](#) to create strong passwords for each of your sites, but you only have to remember one password to access the program that stores your passwords for you. Another service, [Dashlane](#) recently received [praise from the New York Times' David Pogue](#).

"It saves you infinite time and hassle, it's (mostly) free, and it belongs on your computer and phone this very day," he wrote. It's now out in 2.0, and both memorizes your password and automatically logs you in to websites, even with complex logins such as bank accounts.

8. Use common sense.

[Connectsafely.org](#) reminds users that smart Internet habits are the key to password protection:

- **Never share your password with anyone.** The only exception: kids should give theirs to their parents.
- **Don't post it out in the open.** Studies have found that many people still post their password on a sticky note, the organization reports.
- **Don't fall for "phishing."** Never click on a link (even if it appears to be legit) that asks you to log in, change your password or provide any other personal information. It might be a **"phishing" scam**.

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Consumers Feel Stressed By Data Breaches But Fail ...

FTC-0001069

Seniors just turning 65 may be surprised to find their

[Read story](#)



Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Tax Fraud

By Jamie White
November 06, 2013

Share this



:

How does tax fraud occur?

Identity thieves want your tax refund. They can steal bits of your personal information or even your prior year's tax documents, in order to file a fraudulent tax return. The crime may be undetected until you are missing a refund check or the Internal Revenue Service notifies you of a problem.

What are the effects of tax fraud?

Not only can tax fraud thieves steal your refund check, but they can also do serious damage to your good standing with the IRS. If a fraudulent tax return is filed, your official financial information would be wrecked, and you may be facing an audit. It could take years to fix your records with the IRS. Plus, with the stolen information, identity thieves could continue committing identity crimes long after tax season.

The impact:

- ▶ The IRS initiated 1,492 identity theft related criminal investigations last year, a 66 percent increase over 2012.
- ▶ Tax fraud prosecutions and indictments have more than tripled since 2011.

More stories on tax fraud:

[FTC Advice: File Your Taxes Early](#)

[Businesses: Beware of Tax Fraud](#)

[How to E-file Your Taxes for Free](#)

[IRS Responds to Surge in Tax-Related Identity Theft](#)

[Tax Fraud Schemes Target Prisoners and Job Seekers](#)

[Employment ID Theft](#)

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:

FTC-0001071



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Employment Related Fraud

Share this



:



Related articles

- Benefits Fraud

SEE MORE ARTICLES

New laws are making it difficult for illegal immigrants to gain employment—thus entrepreneurial thieves are after your good name to sell it for a high price.

How does employment-related fraud occur?

A criminal background, an illegal status or even a bad work history can make it difficult to find employment. That's why identity thieves are often resorting to employment fraud. In order to pass a background check or employment requirements, a fraudster could use your Social Security number. Even if the employment process requires more than an SSN, employer background checks are often not very thorough. Identity thieves may only need a small amount of additional information.

How could employment related fraud affect my identity?

If an identity thief uses your information for employment purposes, there could be a devastating effect on your employment history and your name. Since incorrect employment will be reported to the Social Security Administration, you may face tax audits, lost tax refunds and errors on permanent government records. They could even use your identity for medical services, home utilities, credit and more. And if you apply for a new job, your employment history may be incorrect and misleading. The effects could take years to resolve.

Statistics

- ▶ Out of all identity theft complaints in 2011, 8% reported to be victims of employment-related fraud.¹
- ▶ Arizona, Colorado, New Mexico and Texas had the greatest percentage of employment-related fraud.¹

¹ Federal Trade Commission. "Consumer Sentinel Network Data Book for January – December 2011."

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For

January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001074

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

▸ Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Loan Fraud

Share this



:



Related articles

- Tax Fraud

SEE MORE ARTICLES

With payday loans, you may not know that someone has used your identity to illegally obtain cash. Thieves can open these types of loans in multiple states, racking up a huge debt using your personal information.

How does loan fraud occur?

Many loaning agencies only require a small amount of information in their lending application process. This makes it easy for identity thieves to use your stolen information—anything from your Social Security number to your banking information—to get a quick loan. Payday loans make it easy for thieves to obtain cash in your name without much verification. Or worse, with enough stolen details, they could open up a legitimate car, home or business loan.

What are the effects of loan fraud?

Since it is typically easy to get a payday loan, many identity thieves choose to take out the maximum amount for their use—and they could even repeat this offense in multiple states. You may not detect the crime until payday loan collectors are aggressively demanding a payment. A larger loan could have an even greater impact—damaging your credit history and building debt.

The impact:

- At an average of \$4,687 in 2011, new loan identity theft cost consumers more than any other identity theft crime.¹

¹ Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Government Documents Fraud

Share this



:



From Social Security cards to birth certificates and driver's licenses, illegally obtaining and selling government documents is big business for thieves.

How does government documents fraud occur?

From illegal immigrants to criminals, there's a substantial customer base for fraudulent government documents. Identity thieves can steal your personal information, such as your Social Security number and address, to create and sell Social Security cards, driver's licenses, birth certificates, identification cards and more.

What are the effects of government documents fraud?

With your identification information, illegal immigrants, criminals or even terrorists can obtain licenses and other government documents. These documents could aid in the smuggling of drugs or illegal immigrants. Or they could use fraudulent identification to gain government benefits, travel state lines or commit crimes. No matter the offense, they could be doing it with your identity.

The impact:

- From April 2006 through July 2010, the Document and Benefit Fraud Task Forces (DBFTFs) generated \$22.6 million in seized assets.¹ Led by the U.S. Immigration and Customs Enforcement, the DBFTFs work towards fighting document and benefit fraud.

¹ U.S. Immigration and Customs Enforcement. "Fact Sheet: Document and Benefit Fraud Task Forces." February 24, 2010. <http://www.ice.gov/news/library/factsheets/doc-bene-fraud.htm>

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

Related articles

- Employment Related Fraud

[SEE MORE ARTICLES](#)

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001078

Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones
- Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Benefits Fraud

Share this



Related articles

- Government Documents Fraud

SEE MORE ARTICLES

In today's healthcare climate, pirated insurance benefits—using your personal information—can earn a high sale price for industrious thieves.

How does benefits fraud occur?

Identity thieves aren't always motivated by financial gain. They instead could gain access to your medical benefits by stealing your insurance information or through employment fraud. Once they've successfully stolen your identity, they could then rack up medical service bills and charges, and in turn, change your medical history.

What are the effects of benefits fraud?

If an identity thief commits benefits fraud, you could unknowingly obtain thousands of dollars in medical expenses. Often the crime goes undetected until you are in need of a legitimate medical service. This could affect your insurance, your taxes, premiums and credit. Even worse, if your medical history and details are changed— such as your blood type or allergies—you could be in physical danger.

The impact:

- The economic impact for medical benefits fraud is \$30.9 billion per year.¹

¹ Arevalo, Christina and Kam, Rick. "The \$234 Billion World Of Medical Id Theft."

View on Hospitals. Multiview Inc. February 13, 2012.

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

[‡] Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach

[Read story](#)



Russian Crime Ring Steals Billions of Passwords, O...
A Russian Crime ring has gathered what may be the

[Read story](#)



What To Do If Your School or Your Child's Sc...

A data breach reported at Butler University in Indianapolis in June exposed

[Read story](#)



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones

▸ Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Bank Fraud



Share this



Related articles

- Loan Fraud

SEE MORE ARTICLES

Nowadays thieves can do more than hold you up at gunpoint to take your money. They can pilfer your bank account information and clean out your savings, before you know it.

How does bank fraud occur?

What better way for identity crooks to get what they want than to go straight to your bank account? With your stolen login and contact information, thieves can break into your bank account, change your information and steal all of your money.

What are the effects of bank fraud?

If an identity thief is able to takeover your bank account, the effects could be extremely detrimental. They could not only clean out your finances, but they could use your stolen information for other banking crimes or open new accounts in your name. They could even wire transfer money overseas, making it extremely difficult to track. Many banks only reimburse up to a certain amount, and it can take months to get your accounts back in order.

The impact:

- Out of all identity theft complaints in 2011, 9% reported to be victims of bank fraud.¹
- Account takeovers cost Americans an average of \$3,692.²

¹ Federal Trade Commission. "Consumer Sentinel Network Data Book for January – December 2011." February 2012.

² Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

[†] Federal Trade Commission. "Consumer Sentinel Network Data Book For

January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Card Skimming Scams on the Rise

When you swipe your card to buy gas or slide

[Read story](#)



What is a Credit Freeze?

A credit freeze gives you the power to seize control

[Read story](#)



Now is the Time to Plan for Retirement

Are you planning for the future? While retirement may seem

[Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001082

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Being Smart When Kids Return to School

Share this



:

Related articles

- Youth at Risk

SEE MORE ARTICLES



Kids love back-to-school season almost as much as identity thieves. And what's not to love? New clothing. New supplies. New schedule. Sometimes even a new school. It's new everything! But all that new stuff means a lot of transactions and exchanging of information—pretty tempting to an identity thief.

From pre-school to college, back-to-school season can be a dangerous time for your children's identity. The best way to protect your kids is to stay informed. Here are six common back-to-school activities that put you and your child's identity at risk.

1. **Sports & Extra-Curricular Activities:** Many after-school activities take place on school grounds, but they may be sponsored by an outside organization with different privacy policies than a school. Make every effort to keep as much information under wraps as possible and ensure your child's information isn't being posted on the organizations websites, game lineups, etc.
2. **Back-to-School Shopping:** Back to school shopping can be fun, as well as a little frantic. But this is not the time to let your guard down. Keep an eye on your credit cards, use cash whenever possible and make sure you're on a secure website and connection when shopping online. Find more information about [credit and debit card fraud](#).
3. **Purchasing Books:** In many colleges, purchasing textbooks requires a student ID number or card. But a student's name and ID number could lead an identity thief to a full profile. Plus, in all the hustle of buying the right books in time for that first class, it's easy to lose track of credit cards and numbers. Before your children start the Fall semester, be sure to talk to them about the importance of keeping these items safe and private. Find out more information about [identity theft and college students](#).

FTC-0001083

4. **Submitting Enrollment Information:** Between birthdates, Social Security numbers and medical documents, schools keep loads of identity information stored for their records. But if they get robbed, hacked or breached, personal information could be compromised. But what can you do? Above all, provide as little information as possible. Keep an eye on what paperwork comes home and what forms go out, making sure this information is delivered securely. If possible, make sure that your child's school keeps its records in a [safe place](#).
5. **Filling Out a FAFSA:** A Free Application for Federal Student Aid (FAFSA) form contains a wealth of personal information. In other words, it's an identity thief's treasure trove. Keep track of communications from FAFSA and shred documents when possible. And be sure not to fall for any fraudulent websites or phishing emails that may be mocking FAFSA documents. Find more information about [phishing](#). Find more information about [counterfeit websites](#).
6. **Knowing Your Rights:** The Protection of Pupil Rights Amendment (PPRA) gives you the freedom to see surveys and instructional materials before they are passed out in the classroom. The Family Educational Rights Privacy Act (FERPA) protects the privacy of your students' information and gives parents and students the option to view those records. Know your rights, and take advantage of them. Monitoring your child's educational records can help you keep your child protected. Find more information about your [federal rights](#).

More articles you might like:



Back to School: How College Students Can Protect t...

So you, or your freshly-minted university student, are headed off

[Read story](#)



Back to School: How to Keep Your Child's Ide...

With Back-to-School time rapidly approaching, parents are soon to be

[Read story](#)



Why Teens Are at Risk for Identity Theft

Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook

Check your Facebook timeline. Chances are that with very little [Read story](#)

Displaying 4 of 6 Results. [Show More Results](#) ▶



Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



5 Ways Seniors are Targeted for Identity Theft

By Beatrice Karnes
June 24, 2014

Share this



Related articles

- Identity Thieves Target Medical Records
- When Identity Theft Hits Home

SEE MORE ARTICLES

Why would identity thieves target senior citizens when most of them are retired? Simple — to get at the wealth accumulated over a lifetime of working and saving.

According to [Pew Research](#), households headed by someone over the age of 65 have 47 times as much net wealth as the typical household headed by someone younger than 35.

Consider Florida with its high concentration of seniors. [Consumer Sentinel Network](#) statistics for 2013 show that Florida has the highest rate of identity theft in the country, with 192 complaints per 100,000 residents and an astounding 340 complaints per 100,000 residents in Miami. In 2014, the state legislature deliberated tougher penalties for identity theft but the effort, [SB1472](#), died in committee.

There are specific ways that seniors are targeted, leading to the opportunity for extra protection:

1. **Medicare ID Theft:** Your Medicare number contains your entire Social Security number, plus some extra letters. Identity thieves go to great lengths to get their hands on your number. Don't routinely carry your card in your wallet. Hospitals must treat you in an emergency so they can get a photocopy of your card later. Once your primary care physician makes a copy of your card the doctor doesn't need to see it again. If they ask for it, tell them to refer to their files — it hasn't changed.
2. **Tax Refund Fraud:** Following retirement, many seniors stop filing tax returns annually as their income drops below the threshold that requires the filing. While refund fraud is a huge problem for all Americans, it hits seniors harder because it takes longer to realize they've been victimized. Filing taxes is free — go through the mental exercise even if it's not required. You may even get a few dollars back.
3. **We're Issuing You a New Card:** The senior receives a phone call from a person who says that he or she is being issued a new Medicare card. The caller just needs to confirm a few things such as date of birth, your old Medicare number, etc. Don't fall for it. A government agency never initiates contact by phone and never asks for personal identifying information — they already have everything on file. Just hang up.
4. **Stolen Mail:** Seniors often do things the same way they've done them for 50 years — such as put outgoing

FTC-0001086

mail in their mailboxes to be picked up by the mail carrier. Swiped mail, incoming or outgoing, contains a wealth of information from credit card numbers and bank account numbers to driver's licenses and unsolicited credit card applications. Get a locking mailbox or a mail slot that drops mail into a secure place. Post outgoing mail at the post office or a USPS mailbox.

- 5. **Fake Funeral Notices:** Due to their advancing age, seniors know more people who die than younger people. This makes them more vulnerable to scams involving death. Earlier this year the **Federal Trade Commission warned of fake emails** purporting to be funeral notices. The recipients were invited to click on a link in the email for more information and to leave condolences. The link downloaded malware onto the victim's computer, making them vulnerable to identity theft.

Beatrice Karnes is a freelance writer. She has many years of experience working behind the scenes at local TV stations in California, Colorado and Wyoming. Most recently, she was an editor for Patch Media, a local news and information consortium of 900 websites nationwide. Beatrice holds a bachelor's degree in journalism from San Jose State University.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Mail Theft

Share this



:



Related articles

- More Than Just a Lost Wallet

SEE MORE ARTICLES

Mail theft is one of the most basic methods available for stealing your personal identity: thieves simply steal your mail. Though many mail thieves are just looking for cash and valuables, identity thieves know your mail contains much more. It contains personal information about your identity and your financial accounts.

How Does Mail Theft Occur?

Whether it's taken from unlocked mailboxes, postal trucks, drop boxes, or mailbox panels, mail theft occurs whenever someone physically takes your mail without your permission. It doesn't matter whether they are stealing the contents (i.e., cash or consumer goods), or whether they're utilizing the personal information contained within to steal your identity—mail theft is a felony.

Information thieves can collect:

- Pre-approved card and other offers
- Social security number
- Telephone numbers
- Email address
- Credit card and bank account information
- Employment history

- Other personal information

What thieves can do with this information:

- Identity theft
- Employment-related fraud
- Loan fraud/payday loan fraud
- Bank fraud
- Benefits fraud
- Tax fraud
- Other identity fraud

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February. 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



USPS Warns of Malware in Phony Email

By Beatrice Karnes
May 28, 2014

Share this



Crooks are phishing for your personal information again.

The **Postal Inspection Service**, the law enforcement arm of the **U.S. Postal Service**, is warning about a phony email that's been reported by victims nationwide. The email claims to be from the USPS and informs the recipient that a package couldn't be delivered. The email contains an attachment or link that, when clicked, installs malware on your computer. The Postal Inspection Service warns the malware "could steal personal identifiers of the customer and compromise the customer's information."

The Postal Inspection Service recommends the following steps if you receive one of the emails:

- ▶ Do not click on the link or open the attachment
- ▶ Forward the email to spam@uspis.gov
- ▶ Delete the email

Fraudsters Also Phoning Victims

Criminals aren't limiting their attacks on consumers to emails — they're also phoning potential victims. Callers use the same scenario as the emails: more information is required to deliver a package. The caller then tries to pry personal identifying information out of the victim.

If you receive one of the calls, the Postal Inspection Service advises:

- ▶ Do not provide any personal identifying information to the caller
- ▶ Hang up
- ▶ Contact your local post office to verify the phone call

Related articles

- [Breach at eBay Prompts Password Warning](#)
- [Counterfeit Website ID Theft](#)
- [Danger of Malware](#)

[SEE MORE ARTICLES](#)

▶ [Contact the Postal Inspection Service at 877-876-2455](#)

The Postal Inspection Service investigation into the fraudulent emails and calls is ongoing.

Beatrice Karnes is a freelance writer. She has many years of experience working behind the scenes at local TV stations in California, Colorado and Wyoming. Most recently, she was an editor for Patch Media, a local news and information consortium of 900 websites nationwide. Beatrice holds a bachelor's degree in journalism from San Jose State University.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001092

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



2 Million Stolen Passwords: What Can You Do?

Share this



Related articles

- How to Avoid Identity Theft at Wi-Fi Hotspots
- How to Pick a Secure Password

SEE MORE ARTICLES

December 7, 2013

Was your password for Facebook, Google or your email just stolen? Would you know if it was?

The security firm Trustwave **just found a file** containing nearly 2 million stolen passwords for email accounts, social media sites and other services. The information was stolen by malicious software that gets onto your personal computer, records your keystrokes and sends the information back to the thieves.

With those passwords, identity thieves can enter your accounts and collect enough other personal information about you to take over your bank accounts, get new credit in your name, steal your tax refund and make your life miserable.

Here's what you should do right away to make yourself more secure:

1. Change Passwords: Facebook and some other companies say they've already changed the passwords of people whose information was in that file. But many people use the same password for all of their accounts, meaning that Facebook password will also get someone into your bank accounts. So change the passwords on sites that contain your personal information, and use different ones for different accounts. Then make a habit of changing them again once every several months.

2. Use Better Passwords: The most popular password in the hackers' file was 123456, according to Trustwave, which makes it way too easy to guess. So pick safer passwords. (See [How to Pick a Secure Password](#).)

3. Check and Protect Your Computer: The software that steals your keystrokes can enter your computer many ways. You can insert a flash drive or DVD that contains it, or download an infected program, or click on a "phishing" email that includes the bad software. Use an anti-virus program -- [PC Magazine offers](#) FTC-0001093

reviews of the best ones -- to protect your computer and check it regularly.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Target: Millions More Customers Were Victims of Data Breach

Share this



January 10, 2014

Target **announced Friday** that the theft of personal information about its customers affected millions more people than it originally reported.

The company first said that the breach happened over a three-week period, from November 27 to December 15, during the prime holiday shopping season and **involved 40 million credit and debit card accounts**. It initially said that only account numbers, customer names and security codes were stolen.

Target has not released information about how the data was stolen, but it now says in an online statement that "the investigation has since determined that the stolen information includes names, mailing addresses, phone numbers or email addresses for up to 70 million individuals."

The company **told Bloomberg News** that it's not yet clear how much overlap there is between the original 40 million card accounts and the 70 million people covered by the new announcement.

"I know that it is frustrating for our guests to learn that this information was taken and we are truly sorry they are having to endure this," Gregg Steinhafel, Target's chairman, president and chief executive officer said in the statement. "I also want our guests to know that understanding and sharing the facts related to this incident is important to me and the entire Target team."

Target has said that customers who suffer fraud because of this breach will not be held liable, and many banks have **posted statements about how they're handling the situation**.

To learn more, visit target.com/databreach.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



FTC Advice: File Your Taxes Early

By Jamie White
January 15, 2014

Share this



While many people consider March and April to be tax time, January and February are the prime season for identity thieves hoping to rake in thousands of dollars.

That's because tax fraud criminals often file false tax returns early using stolen Social Security numbers, hoping to claim thousands of dollars in refunds. In many cases, whoever files first, be it the thief or the legitimate claimant, gets the refund first.

Tax identity theft is the most common form of identity theft reported to the **Federal Trade Commission**. As part of **Tax Identity Theft Awareness Week**, the FTC offers these tips to avoid being a victim:

- ▶ File your tax return early in the tax season, if you can, before identity thieves do. Individuals can start filing their taxes as soon as January 31 this year. If you owe tax, you can still file the return early and then wait to send your payment until April 15.
- ▶ Use a secure Internet connection if you file electronically, or mail your tax return directly from the post office. Don't use unsecure, publicly available Wi-Fi hotspots at places like coffee shops or a hotel lobby.
- ▶ Shred copies of your tax return, drafts, or calculation sheets you no longer need.
- ▶ Respond to all mail from the IRS as soon as possible.
- ▶ Know the IRS won't contact you by email, text, or social media. If the IRS needs information, it will contact you by mail.
- ▶ Don't give out your Social Security number or Medicare number unless necessary. Ask why it's needed,

FTC-0001097

Related articles

- [Businesses: Beware of Tax Fraud](#)
- [IRS Responds to Surge in Tax-Related Identity Theft...](#)
- [Tax Fraud](#)
- [Tax Fraud Schemes Target Prisoners and Job Seekers](#)
- [The Trouble With Tax Returns](#)

SEE MORE ARTICLES

how it's going to be used, and how it will be stored.

- ▶ Get recommendations and research a tax preparer thoroughly before you hand over personal information.
- ▶ Check your credit report at least once a year for free at annualcreditreport.com to make sure no other accounts have been opened in your name.

Tax identity theft victims typically find out about the crime when they get a letter from the IRS saying that more than one tax return was filed in their name, or IRS records show they received wages from an employer they don't know. If you get a letter like this, says the FTC, don't panic. Call the IRS Identity Protection Specialized Unit at 1-800-908-4490 if you get a letter like that, or if you have any reason to believe your Social Security or Medicare number has been compromised. (If you're a LifeLock member, also report it to us at 1-800-LifeLock so we can help.)

More information about tax identity theft is available [from the FTC](#) at and [from the IRS](#).

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Hotels Warn of Credit Card Breach

By Jamie White
February 05, 2014

Share this



Customers of more than a dozen hotels across the United States may have had their credit card information compromised in the latest security breach to unravel in recent weeks.

Independent hotel management company **White Lodging** announced Feb. 3 that it suspects a breach occurred over a nine-month period, from March 20 to Dec. 16, 2013, in restaurants and lounges at 14 of its properties including hotels it runs under the Marriott, Holiday Inn and Westin brands.

The compromised data may have included names, card numbers, security codes and expiration dates. White Lodging urges guests who used or visited the affected hotels during the suspected breach to review their card statements. Customers who suspect unauthorized activity should report it to the issuer of the credit or debit card.

Visa, MasterCard, American Express and Discover offer their credit card holders zero liability for unauthorized charges as long as the charges are reported to them in a timely manner.

Guests should also consider placing a **fraud alert** on their credit files, White Lodging suggests.

The company will offer one year of complimentary personal identity protection services to all affected cardholders. It said in a **news release** that it's working with law enforcement and is reviewing charges at all of the properties it manages.

The hotels affected by the White Lodging breach are:

- ▶ Marriott Midway, Chicago
- ▶ Holiday Inn Midway, Chicago
- ▶ Holiday Inn Austin Northwest, Austin
- ▶ Sheraton Erie Bayfront, Erie, Pa.
- ▶ Westin Austin at the Domain, Austin
- ▶ Marriott Boulder, Boulder
- ▶ Marriott Denver South, Denver
- ▶ Marriott Austin South, Austin
- ▶ Marriott Indianapolis Downtown, Indianapolis
- ▶ Marriott Richmond Downtown, Richmond, Va.

- ▶ Marriott Louisville Downtown, Louisville, Ky.
- ▶ Renaissance Plantation, Plantation, Fla.
- ▶ Renaissance Broomfield Flatiron, Broomfield, Colo.
- ▶ Radisson Star Plaza, Merrillville, Ind.

The hotel incident comes on top of **other retailers experiencing data breaches, including Target** — where up to 110 million of its customers may have had their credit, debit and other personal information stolen over a three-week period late last year.

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results.. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Credit Card RFID Chips Magnets for Identity Thieves

By Marcia Simmons
June 10, 2014

Share this



As an extra layer of security, credit cards and U.S. passports are required to have chips to prevent counterfeiting and identity theft. However, what is intended as a security measure actually opens consumers up to a new form of identity theft. With a special kind of scanner, thieves can skim the information while your cards and passport are still in your wallet.

Known as radio frequency identification (RFID) chips, they transmit an encrypted version of your credit card or passport information to a merchant's or customs agent's chip reader. Though many security **experts say this technology is safe**, one recent identify theft victim would disagree.

Tymikia Jackson was pumping gas at a Georgia filling station, when a woman walked up and asked her for money. Jackson gave her \$20, and then a man who was with the woman insisted on hugging Jackson to thank her. Later, Jackson found that nearly \$3,000 had been charged using her card information, **according to KENS-5**.

Authorities say that the man scanned the information from the RFID-enabled card in Jackson's front pocket during the hug.

Because of the equipment and skill needed to steal and use the stolen information, this type of theft isn't as common as traditional skimming schemes based on the magnetic stripe.

But while it is true that the technology has improved since it was first introduced nearly a decade ago and cases like Jackson's are rare, researchers and "white hat" hackers looking to improve security are **continuously testing for vulnerabilities—and finding them**. And as Jackson's case shows, it isn't always the good guys who find ways past the security measures and encryption.

U.S. credit card companies and merchants face an October 2015 deadline to switch to RFID cards and

Related articles

- 10 Ways to Avoid Identity Theft While Traveling
- What to Do if You Lose a Credit Card

SEE MORE ARTICLES

card readers, if they haven't already. U.S. passports have used this technology since 2007. However, a simpler passport card with a chip that only contains an identification number without the rest of the personal information is available for use when crossing borders by land and sea—for example, to head to Mexico or Bermuda.

Special RFID-blocking wallets are available to thwart would-be thieves. For those who want to keep their wallet or put cards in their pockets, there's **Card Guard**, a protective covering for chipped cards. Some experts say you can improvise protection by wrapping a chipped card in aluminum foil.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Tax Forms from Another State Pose Problem

If you received a letter saying your tax return is

[Read story](#)



Identity Theft Victim? Start Here

You just realized you are a victim of identity theft.

[Read story](#)



P.F. Chang's Continues to Grapple with Breac...

P.F. Chang's China Bistro learned of a security breach involving

[Read story](#)

Displaying 4 of 9 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



When Identity Theft Hits Home

By Marcia Simmons
May 01, 2014

Share this



Many identity theft victims are surprised to find that the individual responsible for stealing their personal information is someone they know.

In fact, nearly one-third of all victims discover a relative was responsible for stealing their identity, according to the Federal Trade Commission.

Last month, Indiana radio personality Kelli Jack-Kelly was accused of using four family members' identities to open credit accounts, [the Indianapolis Star reports](#). Jack-Kelly's father, aunt, father-in-law and mother-in-law are the alleged victims and say they were unaware of the fraud at first, because police say Jack-Kelly had the bills sent to her home.

Unfortunately this situation is all too common.

Tammy Brewer, also in Indiana, stole the identities of her ex-husband and their four daughters, [according to the Post-Tribune](#). She received an 8-year sentence in April. Her ex-husband said in court that she used his Social Security number and then a daughter's to get a job and opened credit cards and student loans using the children's identities. Brewer also forged checks from a man in a nursing home, but he was not related to her.

Seniors and children are sadly the most frequent targets.

Axton Betz-Hamilton [told KTVN](#) in Nevada that she was 19 when she learned her mother had stolen her identity when she was 11— after first stealing her father and grandfather's identities. Betz-Hamilton's mother had already been dead several years before the fraud was discovered.

"My credit report was 10-pages long full of fraudulent credit card entries and associated collection agency

Related articles

- [Cellphone Security: What to Do to Keep Teens Safe](#)
- [States Struggle to Make Birth and Death Certificat...](#)

[SEE MORE ARTICLES](#)

entries," she told KTVN.

Those victimized by family members often pay the debts and choose not to involve the authorities, because they don't want to be responsible for a loved one going to jail or feel pressured by them.

"When someone you don't know steals your identity, it's very impersonal," Mari J. Frank, a lawyer who works with people whose identities have been stolen, said in a [New York Times interview](#). "They just want money. But when it's a family member, it's far more emotionally destructive."

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Retailers Offer Free Credit Monitoring, ID Theft Protection

By Jamie White
January 30, 2014

Share this



Target, Neiman Marcus and Michaels are each promising free credit monitoring and identity theft protection in the wake of recent data breaches.

The Latest from Target

Target's data breach may have affected up to 110 million of its customers. The nation's second largest retailer is offering **one year of free credit monitoring and identity theft** insurance to anyone who shopped at one of its U.S. stores.

Request **an activation code by April 23, 2014 to sign up** for the service. Those who sign up will receive daily credit monitoring, a copy of their credit report, and identity theft insurance.

During **Target's prime holiday shopping season**, Nov. 27-Dec. 15, 2013, hackers stole credit and debit card numbers from the retailer, along with other personal information that may have included names, addresses, phone numbers and email addresses.

Target is also warning people of **phishing scams**, in which fraudsters attempt to collect personal information from people by posing as the retail giant. These scams could appear in the form of emails, texts, phone calls or fake websites.

"We have posted copies of our email communication related to this breach incident to Target.com/databreach, so you can compare any emails you receive to official copies of the emails that Target has distributed," Target's website reads.

Target has a **data breach FAQ section** on its website with more details on scams.

Neiman Marcus Breach

In a letter dated Jan. 22, 2014, Neiman Marcus President and CEO Karen Katz said that the company is "notifying ALL customers for whom we have addresses or email who shopped with us between January 2013 and January 2014, and offering one free year of credit monitoring and identity-theft protection." The **deadline to sign up** for the service is June 15, 2014.

On Jan. 1, a forensics firm found that the company had been breached using malicious software, compromising some customers' debit and credit cards, according to the Neiman Marcus website.

The breach took place between July 16 and Oct. 30, 2013 and may have compromised 1.1 million credit and debit card accounts.

Michaels Investigation

FTC-0001106

Michaels Stores says it's unsure whether a data breach occurred at any of its stores, but the nation's largest arts and crafts retailer has issued a warning to its customers.

"As you may have read in the news, data security attacks against retailers have become a major topic of concern. We recently learned of possible fraudulent activity on some U.S. payment cards that had been used at Michaels, suggesting we may have experienced a data security attack," wrote Michaels CEO Chuck Rubin.

The letter goes on to offer additional information, and says that the store will offer identity protection and credit monitoring services at no cost to its affected customers if the investigation uncovers a data breach.

"If we find as part of our investigation that any of our customers were affected, we will provide information on our website on how to sign up for these services," the letter reads. "We will provide updates on our website as our investigation continues. In the meantime, if you have any questions, please call us toll-free at 1-877-412-7145."

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Target Appoints New Leadership in Wake of Breach

By Jamie White
May 05, 2014

Share this



Related articles

- Target Breach Update: What Your Bank Is Saying

SEE MORE ARTICLES

Nearly five months after **Target suffered a massive data breach**, the company said today that its CEO is stepping down.

"Today we are announcing that, after extensive discussions, the board and Gregg Steinhafel have decided that now is the right time for new leadership at Target," read a **statement on Target's website**.

John Mulligan, Target's chief financial officer, has been appointed as interim president and chief executive officer. Roxanne S. Austin, a current member of Target's board of directors, has been appointed as interim non-executive chair of the board.

Steinhafel, a 35-year veteran of the company, will stay on in an advisory role during the transition. "The board is deeply grateful to Gregg for his significant contributions and outstanding service throughout his notable 35-year career with the company," the statement read. "We believe his passion for the team and relentless focus on the guest have established Target as a leader in the retail industry."

Target also **announced** that starting today, Bob DeRodes will lead its information technology transformation as executive vice president and chief information officer. DeRodes will oversee the Target technology team and operations, with responsibility for the ongoing data security enhancement efforts as well as the development of Target's long-term information technology and digital roadmap.

In a statement released April 29, prior to his departure, Steinhafel said, "Establishing a clear path forward for Target following the data breach has been my top priority. I believe Target has a tremendous opportunity to take the lessons learned from this incident and enhance our overall approach to data security and information technology. Bob's history of leading transformational change positions him well to lead our continued breach responses and guide our long-term digital strategy."

DeRodes has more than 40 years of experience and is a recognized leader in information technology, data

security, and business operations — including working for the U.S. Department of Homeland Security and advising multinational companies.

The company is continuing its active search for a chief information security officer and a chief compliance officer.

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



School Data Breaches Leave Young Children Vulnerable

By Beatrice Karnes
May 07, 2014

Share this



Related articles

- Being Smart When Kids Return to School
- When Identity Theft Hits Home

SEE MORE ARTICLES

Your child's school is required to track each student for a variety of reasons, such as offering free federally-subsidized meals and for charting educational progress. This places a wealth of personal information into the hands of schools— from birth certificates and Social Security numbers, to immunization records and IQ test results.

For information to be useful, it must be shared. Unfortunately, the more it is shared, the more opportunities there are for data security breaches. Your child's information is floating between school district personnel, teachers, administrative assistants and school nurses.

During the 2013-14 school year multiple instances of student data breaches have been reported:

- ▶ Midland, Texas—The names, birth dates and Social Security numbers of 14,000 students were on the hard drive of a laptop stolen from a district administrator's car.
- ▶ Chesterfield, Virginia—130 elementary school students were sent home with the personal information of other students including Social Security numbers, birth dates and birth certificate numbers.
- ▶ Chicago—The names, birth dates and identification numbers of 2,000 students were posted online after the children took a free vision exam at school.
- ▶ Denver—Confidential medical records were on a thumb drive stolen from the car of a school nurse.
- ▶ Louden County, Virginia—A third party vendor accidentally exposed information online including the names, addresses, phone numbers, birth dates and birth places of students. Every school was involved, with the potential to impact 71,000 students.
- ▶ Miami—The FBI reports that a school food service worker and co-conspirators used student Social Security numbers to file about 400 phony tax returns (U.S. vs. Rhim-Grant, et al.)

When the information of students is compromised **it may take years** for them and their families to realize the

FTC-0001111

fallout.

The **Federal Trade Commission (FTC)** recommends that you be proactive about your child's information, "Don't share your child's Social Security number unless you know and trust the other party. Ask why it's necessary and how it will be protected. Ask if you can use a different identifier, or use only the last four digits of your child's Social Security number."

In the Miami case cited above, if the school district had assigned identifying numbers to the students instead of using Social security numbers, the children would not have been victimized.

United States Attorney Wifredo A. Ferrer filed charges against 25 defendants in the Miami area for filing false tax refunds, including the cases involving students. He stated, "These cases serve as a reminder that each and every one of us is a potential victim. While we have a talented and effective team dedicated to fight this fraud, we need everyone—both taxpayers and institutions—to remain vigilant in safeguarding personal identifying information. Protect it as if it were a trade secret."

As a parent, you have the right to review your child's school record. The **Family Educational Rights and Privacy Act (FERPA)** grants you access. Check your child's file for sensitive information and ask for the Social Security number to be removed. Do not provide it in the future.

Protect your children by monitoring their identity as closely as you monitor your own.

Beatrice Karnes is a freelance writer. She has many years of experience working behind the scenes at local TV stations in California, Colorado and Wyoming. Most recently, she was an editor for Patch Media, a local news and information consortium of 900 websites nationwide. Beatrice holds a bachelor's degree in journalism from San Jose State University.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - January 2014

January 26th, 2014

LifeLock chooses Lowe Campbell Ewald as agency of record

January 15th, 2014

ID Analytics Names George Gelly Chief Product Officer





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - February 2014

February 19th, 2014

LifeLock Announces 2013 Fourth Quarter and Year-End Results

February 11th, 2014

National PTA and LifeLock Forge Partnership to Empower Kids and Teens to Be Safe While Using Digital Technology



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - March 2014

March 31st, 2014

ID Analytics Announces ID Score® 9.0 for Advanced Fraud Detection

March 24th, 2014

LifeLock Shares Five Tips to Help Reduce Consumer Risk for the Most Common Tax Scam – Identity Theft

March 18th, 2014

ID Analytics Enhances Customer Experience with New Fraud Detection Solutions for Online Retailers



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - April 2014

April 2nd, 2014

Consumers Can Protect Their Identities and Homes With One Complete, No-Hassle Package





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - May 2014

May 13th, 2014

LifeLock Survey Reveals That 47 % of Consumers Who've Heard of the Heartbleed Bug Have Not Changed Even One Password and May Still Be Susceptible to Hackers



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - June 2014

June 26th, 2014

Newlyweds, New Parents Are Significantly More Likely Than the Average Population to Become Victims of Identity Theft



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - July 2014

July 30th, 2014

LifeLock Announces New Personalized Alerts Across Credit Cards, Checking, Savings and Investment Accounts

July 30th, 2014

LifeLock Announces 2014 Second Quarter Results

July 28th, 2014

First Financial to Offer LifeLock® Identity Theft Protection Services

July 15th, 2014

LifeLock Completes Identity Theft Training for More Than 10,000 Law Enforcement Agents in All 50 States

July 10th, 2014

LifeLock Announces Date of Second Quarter 2014 Financial Results Conference Call



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

[Overview](#)
[Board of Directors](#)
[Management](#)
[Investors](#)
[Press Releases](#)
[Events & Presentations](#)
[Stock Quote](#)
[Stock Chart](#)
[SEC Filings](#)
[Corporate Governance](#)
[Investor FAQ's](#)
[Media](#)
[Legal](#)
[Careers](#)
[Contact Us](#)
[LifeLock in the Community](#)

CALL US AT
1-800-607-
7205

[Send us an email](#)

[Secure login](#)


Press Releases - January 2013

January 31st, 2013

LifeLock Presents Free Identity Theft Summit to Bring Together Law Enforcement Officials in Arizona

January 16th, 2013

LifeLock Presents Free Identity Theft Summit to Bring Together Law Enforcement Officials in Virginia

January 15th, 2013

LifeLock Announces Date of Fourth Quarter and Full Year Financial Results Conference Call

January 8th, 2013

LifeLock to Present at the 15th Annual Needham Growth Conference



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - February 2013

February 21st, 2013

LifeLock and FBI-LEEDA Bring Identity Theft Education to Brevard County

February 8th, 2013

LifeLock to Present at the Goldman Sachs Technology & Internet Conference

February 1st, 2013

LifeLock Goes to Hollywood with the World Premiere of Universal Pictures' Comedy *Identity Thief*





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - March 2013

March 29th, 2013

Designing Spaces™ on Lifetime TV Welcomes LifeLock, Inc. to Show

March 19th, 2013

Less Than One Quarter of Taxpayers Very Concerned about Identity Theft when Filing Returns

March 19th, 2013

ID Analytics Introduces ID Network Attributes For Greater Insight Into Identity Risk

March 13th, 2013

LifeLock Names Key Executives to Further the Fight against Identity Theft



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - ▶ **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - April 2013

April 25th, 2013

LifeLock to Present at the Bank of America Merrill Lynch 2013 Smid Cap Conference

April 9th, 2013

LifeLock Announces Date of First Quarter 2013 Financial Results Conference Call





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - May 2013

May 14th, 2013

ID Analytics to Host 11th Identity And Credit Risk Management Conference





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - Press Releases
 - Events & Presentations
 - Stock Quote
 - Stock Chart

- SEC Filings
- Corporate Governance
- Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - June 2013

June 26th, 2013

LifeLock Names Seth Greenberg as Chief Marketing Officer

June 13th, 2013

ID Analytics and IdentityMind Partner to Reduce Online Fraud and Stop Merchant Account Creation Fraud

June 11th, 2013

Dr. Stephen Coggeshall Named Chief Analytics and Science Officer of ID Analytics and LifeLock

June 10th, 2013

Potential Wedding Crashers: Survey Finds Financial and Technology Surprises in Relationships





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - July 2013

July 24th, 2013

LifeLock Announces Date of Second Quarter 2013 Financial Results Conference Call

July 24th, 2013

ID Analytics Announces ID Score® 8.3 for Advanced Fraud Detection

July 24th, 2013

LifeLock to Present at Upcoming Investor Conferences

July 23rd, 2013

Keynotes, Agenda Set for Advance 2013 Conference

July 9th, 2013

ID Analytics Announces ID Score® Account Takeover 2.0 for Improved Risk Mitigation





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - August 2013

August 26th, 2013

75% of Teens Share Too Much Personal Data, a LifeLock Survey Finds

August 20th, 2013

ID Analytics Names New Chief Scientist

August 12th, 2013

LifeLock Adds Marketing Leader Gary Briggs to Board of Directors

August 1st, 2013

LifeLock Names Villi Ilchev as Executive Vice President of Corporate Development





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - October 2013

October 22nd, 2013

LifeLock Survey Finds Smartphone Users Alarminglly Unaware of Mobile Identity Theft Threats

October 22nd, 2013

Lowe Campbell Ewald Named Advertising Agency of Record for Lifelock



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - December 2013

December 19th, 2013

LifeLock Sponsors Identity Theft Resource Center White Paper on the Paradox of Declining Property Crime Despite Increasing Identity Theft Crime

December 12th, 2013

Leading Identity Theft Protection Company LifeLock Acquires Mobile Wallet Innovator Lemon, Inc.





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - January 2012

January 17th, 2012

Georgia Law Enforcement Invited to Free Identity Theft Summit Presented by FBI-LEEDA and LifeLock

January 12th, 2012

LifeLock's Clarissa Cerda Honored by Arizona Business Magazine and the Association of Corporate Counsel

January 3rd, 2012

Texas Law Enforcement to Begin the New Year with Award-Winning Identity Theft Summit Presented by FBI-LEEDA & LifeLock



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ **Press Releases**

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Press Releases - February 2012

February 28th, 2012

California Shines Spotlight on Identity Thieves during Law Enforcement Training Presented by LifeLock and FBI-LEEDA

February 28th, 2012

LifeLock and FBI-LEEDA Present Law Enforcement Training in Michigan

February 14th, 2012

Tennessee Law Enforcement Invited to Identity Theft Summits in Nashville and Chattanooga, Presented by FBI-LEEDA & LifeLock

February 6th, 2012

LifeLock Partners with Relativity Media on its Upcoming Navy SEALs Action Thriller Act of Valor, in theatres February 24th



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - March 2012

March 14th, 2012

LifeLock Strengthens Market Position through Acquisition of ID Analytics

March 8th, 2012

LifeLock Wins Stevie® Award at the 2012 Stevie Awards For Sales & Customer ServiceSM

March 6th, 2012

Virginia Welcomes Award-Winning Identity Theft Summit for Law Enforcement





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - ▶ **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - April 2012

April 19th, 2012

Michigan Law Enforcement Officials Fight Back Against Identity Theft

April 17th, 2012

Idaho Law Enforcement Invited to Free Identity Theft Summit Presented by FBI-LEEDA & LifeLock

April 11th, 2012

Louisiana Law Enforcement Invited to Free 2-Day Identity Theft Workshop Presented by FBI-LEEDA and LifeLock

April 10th, 2012

LifeLock Offers Identity Theft Protection through Transamerica Employee Benefits to Provide Employers and their Employees Peace of Mind

April 3rd, 2012

LifeLock and ProtectCell Announce Partnership to Further Protect Consumers





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - May 2012

May 31st, 2012

Virginia Police Law Enforcement to Tackle Identity Theft Issues

May 21st, 2012

LifeLock Named Finalist in Several Categories at American Business Awards

May 17th, 2012

El Paso Law Enforcement Fight Back Against Identity Theft in Community

May 15th, 2012

Colorado Law Enforcement Invited to Identity Theft Summit in Thornton, Presented by FBI-LEEDA & LifeLock

May 8th, 2012

LifeLock Wins Communitas Award for Excellence in Community Service





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - June 2012

June 21st, 2012

Summer Travel Schedules Create Opportunities for Identity Theft

June 20th, 2012

LifeLock Wins Stevie® Awards in Annual American Business Awards®, for Sixth Consecutive Year

June 18th, 2012

California Law Enforcement Invited to Free Identity Theft Training in San Francisco and Galt Presented by FBI-LEEDA and LifeLock

June 14th, 2012

LifeLock and FBI-LEEDA Reach Training Milestone: 100 Free Identity Theft Summits for Law Enforcement

June 5th, 2012

LifeLock Presents: Secrets Identity Thieves Don't Want You to Know



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - July 2012

July 23rd, 2012

Free Identity Theft Training Scheduled for July 24th in Auburn, Maine

July 19th, 2012

LifeLock's Award-Winning Solution Offered as Employee Benefit

July 10th, 2012

First Victoria National Bank; First in Nation to Make LifeLock Identity Theft Protection Seamlessly Available to its Customers

July 9th, 2012

LifeLock & FBI-LEEDA Award-Winning Identity Theft Summit Scheduled for Alaska





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - August 2012

August 28th, 2012

LifeLock Files Registration Statement for Proposed Initial Public Offering

August 1st, 2012

LifeLock Brings Texas Law Enforcement Together for Identity Theft Training





Services

\$1M. Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart

Press Releases - September 2012

September 27th, 2012

LifeLock to Present Award-Winning Identity Theft Summit in Utah

September 25th, 2012

LifeLock Delivers Free Identity Theft Training for Oregon Law Enforcement

September 12th, 2012

LifeLock to Present Award-Winning Identity Theft Summit in Indiana

September 10th, 2012

LifeLock names former Yahoo! Executive Hilary Schneider as President

- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart

- SEC Filings
- Corporate Governance
- Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - October 2012

October 18th, 2012

LifeLock Announces Date of Third Quarter Financial Results Conference Call

October 17th, 2012

LifeLock Named Organization of the Year in The 2012 American Business Awards

October 10th, 2012

No title found in javelin-names-lifelock-ultimate-best-in-class

October 2nd, 2012

LifeLock Prices Initial Public Offering



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

[Overview](#)
[Board of Directors](#)
[Management](#)
[Investors](#)
[Press Releases](#)
[Events & Presentations](#)
[Stock Quote](#)
[Stock Chart](#)
[SEC Filings](#)
[Corporate Governance](#)
[Investor FAQ's](#)
[Media](#)
[Legal](#)
[Careers](#)
[Contact Us](#)
[LifeLock in the Community](#)

CALL US AT
1-800-607-
7205

[Send us an email](#)

[Secure login](#)


Press Releases - November 2012

November 27th, 2012

AltaOne Offers LifeLock Identity Protection Services

November 20th, 2012

Based on the Harris/LifeLock Survey More than 48% of Americans are Concerned About the Security of their Personal Information this Holiday Season

November 20th, 2012

LifeLock Introduces 'America's Mayor' Rudy Giuliani As Strategic Advisor to Enhance Consumer Awareness of the Threat of Identity Theft

November 12th, 2012

LifeLock Unveils New Facebook App – 'LifeLock for Life'



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - December 2012

December 11th, 2012

Council for Identity Protection Launches to Examine Key Challenges for the Identity Fraud, Cyber Security and Mobile Markets





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart

Press Releases - January 2011

January 19th, 2011

LifeLock Announces Partnership with Aircraft Owners and Pilots Association to Better Protect Pilots

January 17th, 2011

LifeLock Names Seasoned Executive Chris Power as CFO

January 6th, 2011

LifeLock CEO Todd Davis Keynote Speaker at ASU

January 5th, 2011

More Than 11 Million Records Compromised by Data Breaches in 2010

- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - February 2011

February 17th, 2011

Miami Police Department to Host Award-Winning Identity Theft Summit





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - March 2011

March 29th, 2011

LifeLock Launches Upgraded Website

March 15th, 2011

Identity Theft Awareness Week

March 8th, 2011

Identity Theft Costs Time and Money





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - April 2011

April 28th, 2011

LifeLock Named 2011 Communitas Leadership Winner for Consumer Education

April 27th, 2011

Sony PlayStation Network Breach Leaves Subscribers at Risk

April 21st, 2011

Identity Theft Seminar to Aid Law Enforcement

April 19th, 2011

Identity Theft Seminar to Aid Law Enforcement Officials

April 16th, 2011

How LifeLock Forced the Take-Down of a Malicious Website

April 14th, 2011

LifeLock Aligns with 'America's Health Insurance Advocate®' Cary Hall to Protect Consumers from Identity Theft

April 14th, 2011

Data Breaches Soar in First Quarter. Consumers Often Left Wondering What to Do

April 13th, 2011

Stolen OSDH Laptop May Contain Medical Data of 130,000

April 12th, 2011

Texas Comptroller Breach

April 7th, 2011

LifeLock's Very Odd Case





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ **Press Releases**

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Press Releases - May 2011

May 26th, 2011

Award-Winning Identity Theft Training Set for North Carolina Law Enforcement June 2

May 26th, 2011

Identity Theft a Growing Concern during National Internet Safety Month

May 17th, 2011

LifeLock's Award-Winning Identity Theft Summit Set for May 24 in North Dakota

May 12th, 2011

LifeLock Named Finalist in 14 American Business Awards

May 11th, 2011

LifeLock Receives Gold in Hermes Creative Awards



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - June 2011

June 21st, 2011

LifeLock Wins Stevie® Awards in 9th Annual American Business Awards

June 20th, 2011

Combat Sneaky Cyber Predators Wherever They May Lurk

June 16th, 2011

Citigroup Joins Sony, Epsilon, and Others in 2011 Data Breach List

June 15th, 2011

Nevada Attorney General to Host Advanced, Two-Day Identity Theft Training for Law Enforcement June 22 & 23

June 13th, 2011

Reporting Identity Theft Can Pay Dividends

June 7th, 2011

Understand Your Credit Identity with LifeLock Credit Score Manager

June 1st, 2011

LifeLock Offers 5 Stay-Smart Tips for National Internet Safety Month





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - July 2011

July 19th, 2011

ContentWatch and LifeLock Partner to Protect Children from Identity Theft and Inappropriate Web Content

July 14th, 2011

Montana Law Enforcement Invited to Award-Winning Identity Theft Summit July 19 & July 21

July 13th, 2011

Protection 1 Aligns with LifeLock to Help Protect Consumers against Identity Theft



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

Press Releases - August 2011

August 31st, 2011

Colorado Law Enforcement Invited to Join in the Battle Against Identity Theft

August 24th, 2011

Inc. Magazine Recognizes LifeLock as Fast Growing Private Company

August 24th, 2011

Florida Law Enforcement Learn How to Help Take Down Identity Thieves

August 18th, 2011

Boston Welcomes Award-Winning Identity Theft Summit for Law Enforcement

August 16th, 2011

New York Stock Exchange to Host Identity Theft Training for Law Enforcement on August 16th

August 15th, 2011

National Crime Prevention Council and LifeLock "Take a Bite out of Crime" with Law Enforcement Training

August 11th, 2011

Albany Mayor Gerald Jennings Declares August 14 – 20 as Identity Theft Awareness Week

August 3rd, 2011

LifeLock Wins International Stevie® Award in Eighth Annual International Business Awards

CALL US AT
1-800-607-7205

Send us an email 

Secure login 





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - September 2011

September 28th, 2011

LifeLock & FBI-LEEDA Provide Identity Theft Training for Arizona Law Enforcement

September 22nd, 2011

Stealing Identities in Steel City – Law Enforcement Training Scheduled to Help Combat Crime

September 20th, 2011

Illinois Governor Quinn Declares September 25 – October 1 “Identity Theft Awareness Week”

September 20th, 2011

City of Brotherly Love Area Law Enforcement Scheduled To Receive Identity Theft Training

September 9th, 2011

Free Identity Theft Summit Presented in the Great Lakes State

September 8th, 2011

The Buckeye State Law Enforcement Invited To Free Identity Theft Summit





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - October 2011

October 18th, 2011

Utah Law Enforcement Invited to Free 2-Day Identity Theft Workshop Presented by FBI-LEEDA & LifeLock

October 13th, 2011

LifeLock Command Center and LifeLock Credit Score Manager named Best in Class for Prevention

October 3rd, 2011

Mark Your Calendar: October is National Crime Prevention Month





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

[Overview](#)
[Board of Directors](#)
[Management](#)
[Investors](#)
[Press Releases](#)
[Events & Presentations](#)
[Stock Quote](#)
[Stock Chart](#)
[SEC Filings](#)
[Corporate Governance](#)
[Investor FAQ's](#)
[Media](#)
[Legal](#)
[Careers](#)
[Contact Us](#)
[LifeLock in the Community](#)

CALL US AT
1-800-607-
7205

[Send us an email](#)

[Secure login](#)


Press Releases - November 2011

November 30th, 2011

Report Demonstrates Increase in Identity Theft Results in Greater Cost to Victims

November 29th, 2011

Florida Law Enforcement Invited to Advanced Two-Day Identity Theft Summit Presented by FBI-LEEDA & LifeLock

November 17th, 2011

Connecticut Law Enforcement Learn How To Fight Identity Theft

November 15th, 2011

Kentucky Law Enforcement Learn How To Fight Identity Theft and Investigate Cases

November 8th, 2011

LifeLock Ultimate™ – Ultimate Protection, Ultimate Peace of Mind Consumers Now Offered the Ultimate in Proactive Identity Theft Protection

November 2nd, 2011

LifeLock Named in Lead411 2nd Annual Technology 200 List



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - December 2011

December 8th, 2011

Law Enforcement Spend Day Learning How to Fight Identity Theft and Investigate Cases

December 1st, 2011

Governor O'Malley and Mayor Rawlings-Blake Declare this week (December 4-10) as Identity Theft Awareness Week



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - January 2010

January 1st, 2010

Life Quotes, Inc. Works with LifeLock to Help Better Protect Users' Finances

January 1st, 2010

LifeLock, Inc. Names New Chief Technology Officer

January 1st, 2010

National Financial Wellness Month

January 1st, 2010

LifeLock and FBI-LEEDA host training sessions in various cities across U.S.

January 1st, 2010

Consumers Can Take Control Of Their Identities





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - February 2010

February 1st, 2010

LifeLock Takes Aim at Cybercrime with Norton 360 Security Suite Offer for Members

February 1st, 2010

LifeLock Helps Conserve Personal Information, National Wild Turkey Federation Conserves Wildlife

February 1st, 2010

Georgetown Savings Bank Helps Protect Customers From Identity Theft





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - March 2010

March 25th, 2010

The Celebrity Apprentice Tackles Identity Theft

March 24th, 2010

Tax Season: An Identity Thief's Paradise

March 9th, 2010

LifeLock, FTC and State Attorneys General Agree to Advertising Standards

March 1st, 2010

Tom Ridge Joins LifeLock Board of Directors

March 1st, 2010

Louisiana Law Enforcement Training Summit

March 1st, 2010

LifeLock Adds Senior Executive to Product and Technology Team

March 1st, 2010

National Consumer Protection Week Highlighted with Launch of Identity Smart Book

March 1st, 2010

LifeLock Partners with Folds of Honor Foundation

March 1st, 2010

No title found in census-partnership





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - April 2010

April 28th, 2010

Help Keep Your Identity Safe this Spring

April 1st, 2010

LifeLock Extends Personal Identity Protection With Enhanced LifeLock Identity Alert System





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

[Overview](#)
[Board of Directors](#)
[Management](#)
[Investors](#)
[Press Releases](#)
[Events & Presentations](#)
[Stock Quote](#)
[Stock Chart](#)
[SEC Filings](#)
[Corporate Governance](#)
[Investor FAQ's](#)
[Media](#)
[Legal](#)
[Careers](#)
[Contact Us](#)
[LifeLock in the Community](#)

CALL US AT
1-800-607-
7205

[Send us an email](#)

[Secure login](#)


Press Releases - May 2010

May 27th, 2010

Profiles of Honor: Chief Warrant Officer Erik Mounsey

May 26th, 2010

Profiles of Honor: Staff Sergeant Heath Calhoun

May 25th, 2010

Profiles of Honor: Lieutenant Colonel Greg Gadson

May 24th, 2010

Right To Play Donation

May 21st, 2010

LifeLock Partners With Folds Of Honor Foundation

May 19th, 2010

LifeLock Ranks #1 by TopTenREVIEWS: Identity Theft Protection Leader Receives Gold Award

May 17th, 2010

LifeLock Named As Finalist in 2010 American Business Awards

May 1st, 2010

LifeLock Receives a Best-in-Class 5-star Rating from TopConsumerReviews.com

May 1st, 2010

Leader in Identity Theft Protection Offers Free Nationwide Educational Seminars



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - June 2010

June 7th, 2010

LifeLock and Phoenix Mercury Launch Ultimate WNBA Road Trip Sweepstakes

June 3rd, 2010

National Internet Safety Month

June 1st, 2010

Profiles of Honor: Private First Class Zaneta Adams

June 1st, 2010

Profiles of Honor: Corporal Brock Bucklin



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart

- SEC Filings
- Corporate Governance
- Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - July 2010

July 23rd, 2010

FBI-LEEDA Welcomes LifeLock as DIAMOND Level Corporate Partner

July 12th, 2010

LifeLock Wins International Stevie Award

July 1st, 2010

Reader's Digest Association Better Protects Customers with Leading Identity Theft Protection

July 1st, 2010

QDI Wireless Brings LifeLock Identity Theft Protection to Customers



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - August 2010

August 24th, 2010

LifeLock Receives Top Ten Ranking on Inc. Magazine's Inc. 500 List

August 11th, 2010

Governor Signs Identity Theft Awareness Week Proclamation

August 9th, 2010

Colleges Nationwide Breach Students' Sensitive Information





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - September 2010

September 30th, 2010

LifeLock Presents Free Identity Theft Protection Classes

September 27th, 2010

LifeLock Raises Awareness During National Crime Prevention Month in October

September 21st, 2010

LifeLock Honored as Arizona's 7th Fastest Growing Private Company

September 10th, 2010

Credit Score Manager a New Service Offering

September 1st, 2010

LifeLock LifeLock Honored as One of Arizona's Most Admired Companies





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - October 2010

October 11th, 2010

Free Identity Theft Training Summit to Alabama Law Enforcement

October 6th, 2010

National Cyber Security Awareness Month

October 1st, 2010

Free Identity Theft Training Summit to Missouri Law Enforcement

October 1st, 2010

Free Identity Theft Training Summit to Louisiana Law Enforcement

October 1st, 2010

Law Enforcement Nationwide Discover Best Practices for Combating Identity Theft in the New Year

October 1st, 2010

LifeLock Warns Consumers of Skimming





Services

\$1M. Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - November 2010

November 30th, 2010

LifeLock & FBI-LEEDA Present Advanced Two-Day Identity Theft Training Summit to Nevada Law Enforcement

November 23rd, 2010

M2 Benefit Solutions and LifeLock Partner

November 22nd, 2010

LifeLock & FBI-LEEDA Present Award-Winning Identity Theft Training Summit

November 15th, 2010

Lead411 Announces LifeLock as a Hottest Southwest Company

November 10th, 2010

Award-Winning Identity Theft Training Summit Set for Columbus Law Enforcement





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - December 2010

December 13th, 2010

LifeLock's Educational Priorities Pay Dividends for Consumers, Law Enforcement in 2010

December 6th, 2010

LifeLock Named As Best Place to Work in Valley

December 2nd, 2010

LifeLock Recognized for Corporate Excellence in 2010



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - August 2009

August 30th, 2009

LifeLock Announces Next Generation of Services That Help To Combat Identify Theft

August 1st, 2009

LifeLock Names New Chief Marketing Officer

August 1st, 2009

LifeLock and National Crime Prevention Council Form Strategic Alliance to Help Protect Consumers from Identity Theft



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Overview

Board of Directors

Management

Investors

▸ Press Releases

Events & Presentations

Stock Quote

Stock Chart

SEC Filings

Corporate Governance

Investor FAQ's

Media

Legal

Careers

Contact Us

LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email



Secure login



Press Releases - September 2009

September 1st, 2009

LifeLock, Inc. Wins 2009 ACE Award



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - October 2009

October 8th, 2009

MENTOR Celebrates National Crime Prevention Month with Success of SafetyNET Program

October 1st, 2009

NOVA Launches Identity Theft Task Force

October 1st, 2009

LifeLock, Inc and Arthritis Foundation Team Up





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

- Overview
- Board of Directors
- Management
- Investors
 - **Press Releases**
 - Events & Presentations
 - Stock Quote
 - Stock Chart
- SEC Filings
- Corporate Governance
- Investor FAQ's

- Media
- Legal
- Careers
- Contact Us
- LifeLock in the Community

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Press Releases - November 2009

November 3rd, 2009

Cabela's Inc. Offers Customers Identity Protection from LifeLock

November 1st, 2009

Phi Kappa Phi Aligns with LifeLock

November 1st, 2009

LifeLock's Expanded Identity Theft Protection Service Launches Successfully





The background of the entire page is a dense field of shredded paper, rendered in a monochromatic red color. The shreds are of various lengths and orientations, creating a textured, chaotic appearance. The central text is set against a lighter, circular gradient that fades into the surrounding red paper.

IDENTITY SMART:

**A Guide for Consumers
to Help Protect Against
Identity Theft**

IDENTITY ALERT:

The Fight to Defend Your Identity and Personal Information

A frightening crime with an untraceable weapon, identity theft is creating anxiety across the country. In fact, 1 incident every 3 seconds of identity fraud is occurring in households throughout America¹. This horrible and personal crime can cause Americans to live their lives in fear—opening each monthly bank statement with bated breath.

With the anonymity of computer keyboards and high level technologies, imposters, and hackers can commit identity-related crimes on any unsuspecting victim, from anywhere in the world. With the nine simple digits of a Social Security number, or an electronic scan of your debit card, an identity thief can wreak havoc on your personal, legal or financial life for months or years—and sometimes with no detection at all.

It falls to you to raise your level of identity theft awareness—and to help defend yourself against a crime that can drain your time, your resources, and your good name.

¹ www.identitytheftassistance.org “Research and Statistics” Identity Theft Assistance Center, 2012.



WHAT IS IDENTITY THEFT?

According to the U.S. Department of Justice²:

“Identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in some way that involves fraud or deception, typically for economic gain.”

In short, identity theft can be defined as the fraudulent use of personal information to commit crimes. These crimes can often end in tax fraud and credit fraud, but are also perpetrated for insurance, medical or legal purposes.

² www.Justice.gov “What Are Identity Theft and Identity Fraud?”

FTC-0001229

IDENTITY THEFT: THE NUMBERS

How the Facts and Figures Affect Your Day-To-Day Life

The prospect of a faceless online hacker stealing your personal identity information may not resonate with you at first—at least not until you get a frightening look at the numbers that tell the true story of identity theft.

Identity Theft was the number one complaint category for the past 13 years.³

The facts and figures compiled below shed some light on the growing problem:

- There were 12.6 million adult victims of identity theft in 2012⁴
- 1 in 20 consumers were victims of identity theft in 2012⁴
- The total loss in new account fraud, where a criminal uses a victim's personal information to open a new credit card or loan, reported just under \$10 billion in 2012.⁴
- Credit card fraud accounts for two-thirds of all ID theft⁵
- 1 in 4 data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.⁵
- Government documents/benefits fraud (46%) was the most common form of reported identity theft, followed by credit card fraud (13%), phone or utilities fraud (10%), and bank fraud (6%). Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (2%).³
- Consumers reported paying over \$1.4 billion in one million fraud-related cases. The median amount was \$535. Of these fraud related cases 38% were contacted through email, 34% by telephone, and 9% through mail.³

³ FTC. "Consumer Sentinel Network Data." January-December 2012.

⁴ Sullivan, B. (2012). ID Theft on the rise again: 12.6 million victims in 2012, study shows. NBC News

⁵ www.identitytheftassistance.org "Research and Statistics" Identity Theft Assistance Center, 2012

TO CATCH A THIEF

What You're Leaving Behind, and How Identity Thieves are Following the Trail

At work, on the town or sitting at home, you may be most vulnerable to identity theft when you least expect it. The following are some of the ways that identity thieves commit their crimes:



Phishing:

When fake emails are so well produced, they can be almost impossible to discern from legitimate ones. If you get tricked into clicking a link or submitting information through a fake email, you can find yourself on a long road to losing your passwords, your accounts and your data.



Online Shopping:

Consumers beware: shopping online has become a phenomenon around the world, and it's become one of the easiest ways to have your information stolen. Whether you're shopping at duplicate retail sites or through unsecured payment systems, your credit/debit cards could be at risk.



Data Breaches:

If you store personal information with any financial or business organization—even a huge insurance or medical corporation—your files could be compromised in a large-scale data breach.



Malware and Viruses:

With thousands of new viruses emerging daily, your computer and your information can be hacked through any website, Internet program or file sharing application.



Keystroke Logging:

On public computers, gas station pump displays and ATM keypads, criminals and hackers can install technologies to trace the buttons you press as you enter your card numbers, passwords and PINs.



P2P File-Sharing:

File sharing sites like Bearshare and Frostwire connect millions of users across the world — and they also connect unsuspecting music fans with viruses and open connections to unsecured networks.

Vishing:

Just as you can be tricked into divulging personal or protected information through a text message or website, you should also be wary of giving away information over the phone or through voice messages.

**Shoulder Surfing:**

Technology can make stealing identities easier than ever before, but old-fashioned ways are still just as effective at manipulating unsuspecting victims. Through shoulder surfing, any identity imposter can stand behind you with a camera—or even their own eyes—and watch as you enter passwords, personal identification numbers or private information.

**Dumpster Diving:**

Though not the most glamorous of identity stealing techniques, many criminals and fraud-minded imposters have taken to sorting through garbage to find old bills, recent receipts and other discarded personal information that can be easily stolen.

**Change of Address:**

This is a classic identity theft technique—thieves change the address where you receive mail and divert your personal information into the wrong hands.

**Mail Theft:**

Less creative than the change of address method, identity thieves will often simply search for unlocked or unwatched mailboxes, and rip the mail directly from the box itself—often in search of what can be found on credit card statements and tax forms or financial and personal information.

**Stolen Wallet:**

While some thieves might be after your wallet or purse for the money inside, many others will be more interested in the credit cards, Social Security card and other personal identification that you keep inside.

**ATM Overlays:**

Hidden from the untrained eye, thieves install these devices at ATM machines and gas pumps to steal your account information when you insert your card, and transmit it to a nearby computer.



THE OTHER SIDE OF IDENTITY THEFT

Out For More Than Just Money, Identity Thieves Can Take Advantage of Your Medical or Criminal History

When identity imposters decide to go after your PINs, passwords and personal information, they are not always simply trying to drain your bank accounts. They may be looking for something much more specific, and for something that can sacrifice your good name and your future plans.

Medical Identity Theft

You may not notice that your medical identity has been stolen until it comes time for you to receive medical treatment or make a claim on your health insurance. With this kind of theft, imposters will use your name or insurance information to get medical coverage that they may not be able to afford.

Criminal Record Identity Theft

One of the scariest forms of identity theft is when criminals go after your government records. Thieves could use your information to apply for a job, avoid paying a traffic ticket or dodge arrest.

Social Security Identity Theft

When your Social Security number is stolen by an identity thief, they can use the information to create new Social Security cards, access a number of public records or steal your name and personal information completely—assuming your identity.

Tax-Related Identity Theft

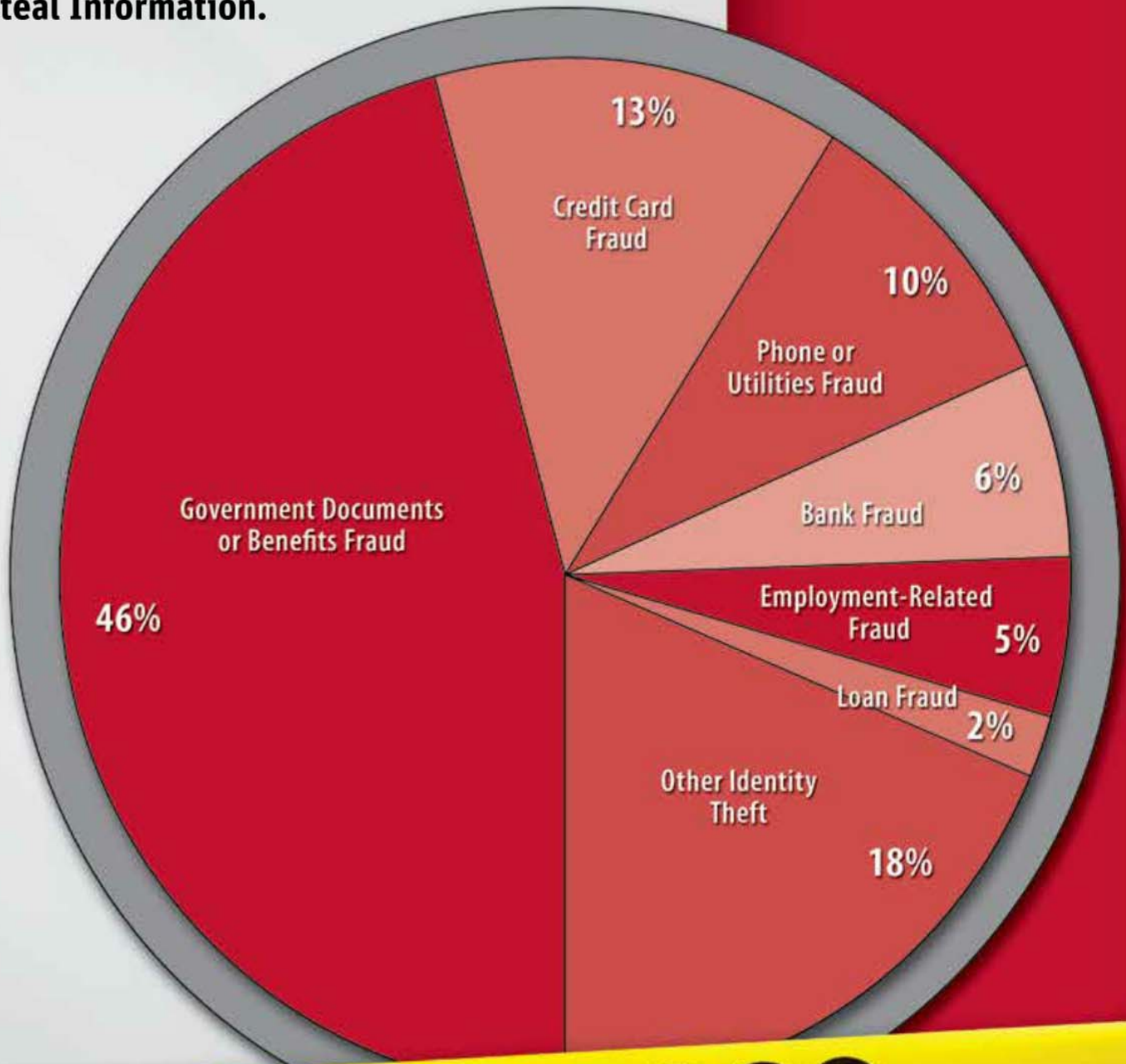
Using a stolen Social Security number, identity thieves can file fraudulent tax returns and receive refunds before you even file.



CRIME SCENE

HOW IDENTITY THIEVES ARE STEALING YOUR IDENTITY

Based on FTC Complaints in 2012³, These Are The Most Common Ways Thieves Steal Information.



DO NOT CROSS

³ FTC. "Consumer Sentinel Network Data." January-December 2012

HELP STOP IDENTITY THEFT BEFORE IT HAPPENS

Follow These Precautions and Protection Tips To Set Up a Line of Defense Against Imposters

In the Mail

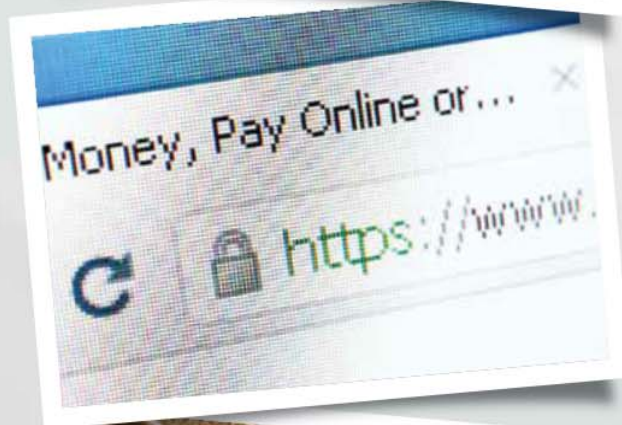
- Avoid placing outgoing mail into unlocked curbside mailboxes.
- Add a slot or a lock to your mailbox at home to prevent access to your private mail.
- Do not write account numbers or personal information on the outside of your envelopes.
- Have the post office hold your mail if you will be leaving town for more than a day or two.

Shopping Online

- Make sure you are doing business or shopping on a secure site before you provide any information. Make sure the site features a lock in the search bar and uses an “https” address.
- Check your billing statements for the company you purchased from to verify the correct amount and the correct purchase information.
- Avoid shopping from public Wi-Fi hotspots.
- Strengthen your shopping website passwords before making any purchases, and be sure to share only the necessary information when creating a login account or page.

Credit and Debit Cards

- When possible, use credit cards instead of debit cards. If your information is stolen from a debit card, an imposter can drain the cash from a checking or savings account—instead of running up your bill on a credit card.
- Make sure that cashiers swipe your credit or debit cards in front of you, and are not swiping them multiple times or through separate machines.
- Check your entire statement every time you receive it in the mail for your debit card or credit card, and be sure to account for every purchase or withdrawal. If banking online, check your statements as often as possible.
- Cancel your card immediately if you notice any suspicious charges or activity.
- Do not carry more debit or credit cards than are absolutely necessary.



FTC-0001235

At the Bank

- Use traveler's checks when possible, which are more difficult to duplicate than personal checks.
- Investigate if you are receiving late statements or late correspondences from your bank.
- Avoid giving personal information over the phone to anyone who claims they are working for a bank or credit card company (unless you previously initiated the contact).
- Use direct deposit when possible to avoid having a check that can be stolen from a payroll department or from the mail.

In Your Wallet/At Your Home

- Invest in a cross-cut shredder for all of your personal, financial or legal records, documents or correspondences. Throwing them away before shredding can leave them prone to dumpster diving imposters.
- Do not carry your Social Security card in your wallet or your purse. Keep it in a safe place at home, and only bring it out when you need it.
- Retrieve your mail promptly, and be sure to investigate if your mail is irregularly late or misses a day.
- Keep your wallet and purse secured when you are out in public, and avoid carrying more identifying personal information than is necessary.

The Last Line of Defense

- Use safe Internet passwords with a combination of letters and numbers. Do not make the passwords too obvious, use them for too many accounts, or keep them written in plain sight.
- Do not give your credit card information over the phone, unless you made first contact with the company.
- Be suspicious of any unexpected emails asking for personal information.
- Destroy the hard drive of your computer if you are selling it or discarding it. Beyond just erasing the hard drive, it should be physically destroyed.
- Safeguard your personal information at all costs, and educate yourself as much as possible about the many scams, imposters, hacks and schemes that are used to procure personal information.



FTC-0001236

HOW TO PICK UP THE PIECES AFTER IDENTITY THEFT

If You're the Victim of an Identity-Related Crime, Here's How You Can Begin to Repair the Damage

Step 1: Contact the Police

Instead of sitting stunned or helpless after an identity crime is discovered, you should take action right away. Start by contacting your local police or sheriff's department. Prepare and provide as much information as possible about what may have led to the identity theft.

Once your report is filed, you should be sure to do the following:

- Report the crime to your state law enforcement (to take advantage of recently toughened state laws regarding identity crimes)
- Obtain a copy of the police report to pursue your case with creditors
- Notify local authorities in the location where your identity was likely stolen



Step 2: Check Your Bank Statements and Balances

Your bank accounts should be the first place that you turn once a breach is detected.

Timing is important when it comes to protecting your savings, and taking the right steps can keep you from losing hundreds or thousands of dollars.

- Close your account right away and place stop payments on any stolen checks.
- Ask the bank to activate its check verification service to prevent identity imposters from cashing checks on your account
- Contact the Shared Check Authorization Network (800-262-7771) to find out if fraudulent checks are being passed in your name
- Order a free copy of the ChexSystems report that lists checking accounts opened in your name. ChexSystems, Inc.: 1-800-428-9623 or www.consumerdebit.com
- Contact businesses that accepted bad checks and report that you are a victim of identity theft.

If you think the fraud may exist beyond your current account—and an identity thief may have opened a new account in your name—contact your bank's consumer reporting service to close the account before it is too late.

Step 3: Contact the Credit Reporting Agencies

Because many identity thieves are looking to take advantage of open lines of credit, the three major credit reporting agencies should play a large role in helping you recover from your stolen identity.

Consumers can receive a free credit report yearly by visiting www.annualcreditreport.com. Monitoring your credit report will display all information about your credit, allow you to dispute any discrepancies, and give you notification if your credit is being used without your permission.

You should contact one of the reporting agencies as soon as possible to have your credit account flagged with a fraud alert. This agency is then required by law to contact the other two. To contact the three major agencies, use the following numbers:

Equifax:	800-525-6285	www.equifax.com
Experian:	888-397-3742	www.experian.com
TransUnion:	800-680-7289	www.transunion.com

Once you contact an agency:

- You can place an alert on your accounts for seven years after any identity theft
- You will receive two free credit reports within 12 months after your identity theft.
- A security freeze: a freeze can be placed on your credit by visiting any of the above credit reporting agencies.

If you suspect you are a victim of identity theft, each credit reporting agency has the option to place a free 90 day fraud alert on your account. Communication will be received from each credit reporting agency if any activity occurs on your credit.



FTC-0001237

Step 4: Connect with Your Creditors

Your creditors can be hit by identity theft as hard as you are, and it will be up to you to notify them as soon as possible of any suspicious activity on your account. The quicker you act, the easier the resolution will be.

You should contact your creditor's fraud department the second you discover any unauthorized charges, and you will be able to limit the charges that you are responsible for paying.

Step 5: Report the Details of Your Case to the Federal Trade Commission (FTC)

The national authority on identity theft and identity-related crimes, the FTC maintains an extensive database used to track, stop and catch identity thieves around the United States. You can contact the FTC through their toll-free hotline at 877-IDTHEFT www.ftc.gov.

STAY SECURE WHEN REPORTING YOUR IDENTITY THEFT

- Report the theft as soon as possible to ensure that you and your personal information are protected.
- Keep a copy or record of any and all correspondence with the authorities, your financial institutions and any credit reporting agencies.
- Avoid using originals of any personal documents when possible; use notarized and certified copies instead.
- Follow-up with all requests and actions, and be persistent in clearing your name and securing your information.

VICTIM ASSISTANCE

Contact the National Organization for Victim Assistance if you are a victim of identity theft for additional assistance at www.trynova.org



60 East Rio Salado Parkway
Suite 400
Tempe, AZ 85281

1-800-543-3562

LifeLock.com

For more information and resources,
please visit: [www.LifeLock.com/
about/lifelock-in-the-community](http://www.LifeLock.com/about/lifelock-in-the-community)



FTC-0001239

Identity Smart Educator Resource Guide: Overview and Outline

Complement to the LifeLock
*Identity Smart: A Guide for Consumers
Against Identity Theft*

Provided to you in partnership with



Partnerships

CyberWatch is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College and funded by a grant from the National Science Foundation (NSF). The CyberWatch mission is to increase the quantity and quality of the information assurance (that is, cybersecurity) workforce.

The CyberWatch K12 Division extends the CyberWatch Mission to the K12 Community. Its mission is to advance cybersecurity education by leading collaborative efforts to strengthen the national cybersecurity workforce.

Educational Technology Policy, Research and Outreach (ETPRO), a research and development organization located in Maryland, connects educational technology policy and research to instructional practice. ETPRO brings more than two decades of experience in the educational community, and more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and conducting educational technology policy analysis. ETPRO's expertise is founded on a combination of classroom practice across K-16 tied with a solid research base.

ETPRO originated from the Educational Technology Outreach division of the College of Education, at the University of Maryland, and in 2007 was founded as an entrepreneurial entity committed to quality education for all learners, targeting the effective use of cutting edge technology in formal and informal educational settings to increase interest in Science, Technology, Engineering and Mathematics (STEM) fields. The fundamental gap between technology use and understanding of proper practices, lead ETPRO to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3[®]) initiatives.

C3 Conference is a high quality professional development event for educators in Maryland and the mid-Atlantic region. The core mission of the C3[®] Conference is to inform the educational community about the ethical, legal, safety, and security implications of technology use and illustrate how educators and parents can apply these concepts to their own setting.

LifeLock, Inc. (NYSE:LOCK) is a leading provider of proactive identity theft protection services for consumers and identity risk assessment and fraud protection services for enterprises. Since 2005, LifeLock has been relentlessly protecting identities by providing consumers with the tools and confidence they need to help protect themselves from identity theft and manage their credit. In October 2012, Javelin Strategy & Research named LifeLock Ultimate™ a "Best in Class Overall" identity theft protection solution and also named it "Best in Detection." In March 2012, LifeLock further demonstrated its commitment to combating identity fraud with the purchase of ID Analytics, Inc., a leader in enterprise identity risk management that provides visibility into identity risk and credit worthiness. ID Analytics, Inc. currently operates as a wholly owned subsidiary of LifeLock, Inc.

Overview

Identity fraud is the fastest-growing category of Federal Trade Commission (FTC) complaints. In 2012, 12.6 million adult Americans fell victim to identity theft.

Children make prime targets for identity thieves specifically because they have no credit history and thus, clean credit reports. Also, because parents don't think to check their children's credit histories, the theft can continue unchecked for over a decade. Police agencies are reporting that children are now the fastest growing segment of identity theft victims. Identity thieves will use children's identities to take out loans and lines of credit they never intend to repay and to establish an identity so they can obtain things like jobs or a driver's license.

Federal Trade Commission. "Consumer Sentinel Network Data Book for January – December 2012." February 2013.
Javelin Strategy & Research. "2013 Identity Fraud Report." February 2013

Outline

SECTION ONE: SURVEYS AND MATERIALS

A. Identity Smart Educator Resource Guide: Surveys and Materials

a. Unit Overview:

This content is designed to provide educators with the means to explore with students the topic of identity theft and the cyberethics, safety and security strategies associated with it. Students and educators will begin to recognize and internalize the importance of assessing and identifying dangers of identity theft, practicing strategies to minimize the risk and formulating plans and next steps for minimizing the risk of loss in the event of an identity theft.

B. Objectives:

a. Upon completion of these lessons and presentations, students will be able to:

- Assess the dangers of identity theft and identity fraud.
- Identify how identity thieves obtain personal information.
- Explain what identity thieves can do with an individual's personal information.
- Practice methods to minimize the risk of identity theft and identity fraud.
- Recognize the warning signs of identity theft and identity fraud.

C. Materials:

a. Baseline and Post-Unit Surveys

To begin the content unit on identity theft, you may wish to administer to students the baseline survey. This survey will help you gauge your student's prior knowledge and experiences surrounding the topic of identity theft. A post-unit survey, similar to the baseline survey is also included, and can help you measure changes in student knowledge. Answers keys are provided.

D. Unit Materials

a. Three baseline and post-unit surveys are included for three different grade bands:

- Elementary/Early Middle School
- Middle and High School
- High School/PTA and Educator Audiences

b. Ice Breaker Scenarios

c. Two case studies, entitled *Security in Cyber Space*,

- Recommended for use with middle/high school and adult level audiences.
- The case studies provide an identity theft related vignette that introduces the unit content and helps the attendees to understand why this topic is important.

d. *Parent take home materials* are included and can be used with all age groups.

e. *References* are also included to help access other identity theft stories in the news.

f. The PowerPoint and case studies can be used separate from or with any of the unit's other activities.

- E. How to Begin:
 - 1. View the materials and the Identity Smart Curriculum PowerPoint.
 - 2. After determining the audience level and format structure, decide on the activities you would like to include. For adults, the open discussion with the PowerPoint is usually enough.
 - 3. The case scenario and PowerPoint is suggested for upper age students. The hands-on activities are suggested for younger audiences.
 - 4. Baseline and follow up surveys are always recommended if time allows.

SECTION TWO: GOALS, DEFINITIONS, GAMES

A. Identity Smart Educator Resource Guide: Goals, Definitions, Games

This series of activities are designed to help reinforce the concepts discussed and provide a multi-approach to presenting the concepts and information.

Grade: 6-12

Content Areas: Technology, Business Education, Language Arts, Library Media

Time: 90 minutes (can be broken into two 45 minute periods)

B. Introductory Activity: Understanding Your Identity

- a. The educator will call students by their wrong name to introduce the topic of identity. This will lead to a discussion which will define identity, identity theft, and identity fraud.

C. Activity 1: Real People, Real Scenarios

- a. The educator will introduce the terms and definitions to the students.
- b. The students will play a game where they match the scenario to the term. By matching the identity theft terms, it will create an understanding of how their behavior can compromise the identity information of others.

D. Activity 2: The Big Picture

- a. The educator will present a PowerPoint which summarizes the *Identity Smart: A Guide for Consumers Against Identity Theft* content.

E. Activity 3: Solutions

- a. The students will play a BINGO game called ID SMART which will reinforce the terms while helping students to brainstorm preventative measures which will protect their identity information.

F. Materials

- a. Identity Smarts Curriculum PowerPoint
- b. *Identity Smart: A Guide for Consumers Against Identity Theft*
- c. Handout: Identity Theft Terms
- d. Handout: Real People, Real Scenarios
- e. Handout: ID SMART Bingo Sheet

Identity Smart Educator Resource Guide: Goals, Definitions, Games

Complement to the LifeLock
*Identity Smart: A Guide for Consumers
Against Identity Theft*

Brought to you in partnership with



CyberWatch is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College and funded by a grant from the National Science Foundation (NSF). The CyberWatch mission is to increase the quantity and quality of the information assurance (that is, cybersecurity) workforce.

The CyberWatch K12 Division extends the CyberWatch Mission to the K12 Community. Its mission is to advance cybersecurity education by leading collaborative efforts to strengthen the national cybersecurity workforce.

Educational Technology Policy, Research and Outreach (ETPRO), a research and development organization located in Maryland, connects educational technology policy and research to instructional practice. ETPRO brings more than two decades of experience in the educational community, and more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and conducting educational technology policy analysis. ETPRO's expertise is founded on a combination of classroom practice across K-16 tied with a solid research base.

ETPRO originated from the Educational Technology Outreach division of the College of Education, at the University of Maryland, and in 2007 was founded as an entrepreneurial entity committed to quality education for all learners, targeting the effective use of cutting edge technology in formal and informal educational settings to increase interest in Science, Technology, Engineering and Mathematics (STEM) fields. The fundamental gap between technology use and understanding of proper practices, lead ETPRO to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3[®]) initiatives.

C3 Conference is a high quality professional development event for educators in Maryland and the mid-Atlantic region. The core mission of the C3[®] Conference is to inform the educational community about the ethical, legal, safety, and security implications of technology use and illustrate how educators and parents can apply these concepts to their own setting.

LifeLock, Inc. (NYSE:LOCK) is a leading provider of proactive identity theft protection services for consumers and identity risk assessment and fraud protection services for enterprises. Since 2005, LifeLock has been relentlessly protecting identities by providing consumers with the tools and confidence they need to help protect themselves from identity theft and manage their credit. In October 2012, Javelin Strategy & Research named LifeLock Ultimate™ a "Best in Class Overall" identity theft protection solution and also named it "Best in Detection." In March 2012, LifeLock further demonstrated its commitment to combating identity fraud with the purchase of ID Analytics, Inc., a leader in enterprise identity risk management that provides visibility into identity risk and credit worthiness. ID Analytics, Inc. currently operates as a wholly owned subsidiary of LifeLock, Inc.

Identity Smart Educator Resource Guide: Goals, Definitions, Games

This series of activities are designed to complement the LifeLock *Identity Smart: A Guide for Consumers Against Identity Theft*.

Grade: 6-12

Content Areas: Technology, Business Education, Language Arts, Library Media

Time: 90 minutes (can be broken into two 45 minute periods)

Introductory Activity: Understanding Your Identity

- The educator will call students by their wrong name to introduce the topic of identity. This will lead to a discussion which will define identity, identity theft, and identity fraud.

Activity 1: Real People, Real Scenarios

- The educator will introduce the terms and definitions to the students.
- The students will play a game where they match the scenario to the term. By matching the identity theft terms, it will create an understanding of how their behavior can compromise the identity information of others.

Activity 2: The Big Picture

- The educator will present a PowerPoint which summarizes the *Identity Smart: A Guide for Consumers Against Identity Theft* content.

Activity 3: Solutions

- The students will play a BINGO game called ID SMART which will reinforce the terms while helping students to brainstorm preventative measures which will protect their identity information.

Materials

- Identity Smarts Curriculum PowerPoint
- *Identity Smart: A Guide for Consumers Against Identity Theft*
- Handout: Identity Theft Terms
- Handout: Real People, Real Scenarios
- Handout: ID SMART Bingo Sheet

Introductory Activity: Understanding Your Identity (10 minutes)

The educator will call students by the wrong name to introduce the topic of identity. This will lead to a discussion which will define identity, identity theft, and identity fraud. The educator can modify the activity to fit the class needs.

Objective:

- The students will define “Identity,” “Identity Theft,” and “Identity Fraud.”

Activity:

1. The instructor begins by calling a student by the wrong name. If the student does not react, then the instructor should continue calling students by the wrong name until the students react.
2. The instructor should ask questions about why the students were reacting when they were called by the wrong name and what the consequences of that could be.

Questions include:

- a. How do you know this is (student name here)?
- b. Why can't I call him/her (wrong student name here)?
- c. Why is it so important that I call him/her by the correct name?
- d. What could happen if I didn't call him/her by the correct name?

These questions should lead the students to the conclusion that your name is an integral part to your identity and that problems can occur if we don't use correct names. Grades can be assigned incorrectly, report cards can be given to the wrong person and the nurse can give you the wrong medicine without having proper identification.

3. Ask students to define “Identity”
The collective aspect of the set of characteristics that make you who you are.

Return to the original discussion about the student and ask the other students to describe that student's identity. In other words: How do we know (student name) is who they claim to be?

- a. We know him/her
 - b. We have gone to school with him/her for a long time
 - c. We have lived on the same street with him/her
 - d. He/She told us that is his/her name
4. Ask students what type of information verifies their identity.
 - a. Social Security Number
 - b. Date and Year of Birthday
 - c. Parent or Student's Bank Account Numbers and Information
 - d. Addresses (Current and past addresses)
 - e. Phone Numbers
 - f. Mother's Maiden Name
 - g. Health Insurance Information
 - h. Usernames and Passwords for Email or Online Accounts
 - i. Parent's Tax Information
 - j. Pet's names
 - k. Parent's Anniversary

5. Ask the students how businesses and organizations verify we are who we say we are?
 - a. Picture Identification (example: driver's license or membership card)
 - b. Credit Card
 - c. Social Security Card
 - d. Passport
 - e. Birth Certificate

6. Ask the students if they have ever heard of "Identity Theft?" Ask them to hypothesize a definition.
All types of crime in which someone wrongfully obtains another person's personal data in some way that involves fraud or deception.

7. Ask the students if they have ever heard of "Identity Fraud?" Ask them to hypothesize a definition.
When someone who has obtained another's identity by fraud or deception then uses the identity for a criminal purpose.

8. Ask the students if they have ever heard of anyone faking or stealing any of these items
 - a. Most kids will have heard how under-age persons have used fake identifications such as driver's licenses.

9. Inform the students that they will be discussing "Identity Theft" and "Identity Fraud" and eventually be brainstorming ways they can proactively protect themselves and the people they know from identity theft.

Activity 1: Real People, Real Scenarios (35 minutes)

The educator will introduce the terms and definitions to the students. The student will be given a scenario and asked to match it with a corresponding “Identity Theft” term. The educator can modify the activity to fit the class needs.

Objective:

- The students will play a game where they match the scenario to the term. By matching the identity theft terms, it will create an understanding of how their behavior can compromise the identity information of others.
1. Preparation: Make copies and distribute the “Real People, Real Scenarios” matching game handout.
 2. Using the PowerPoint presentation, discuss and review the “Identity Theft Terms.” Students may write down each definition in the space provided in the “Real People, Real Scenarios” matching game handout.
 3. The educator will select 10 terms (at their discretion) from the “Identity Theft Terms” document and chose one of the scenarios illustrating the specific term to be used in the game. Each term has two different scenarios to choose from. One scenario is meant to be a little more difficult than the other. The educator can choose the scenario based on the level of class knowledge.
 4. The educator will start the game by reading the first (of 10) chosen scenarios. Each scenario is marked with a letter that should be read along with the scenario. The student will match the scenario with the term on their handout in the space provided. Since the educator is only giving scenarios for 10 terms, there will be terms leftover with no letter/match.
 5. Once all scenarios have been read, ask the students to pass their paper to the student directly behind them. The educator will read the correct answers aloud and the students will grade each other’s papers.

Identity Theft Terms

[Intro to Identity Theft]

Definition	Scenario 1	Scenario 2
<p>Identity: The collective aspect of the set of characteristics that make you who you are.</p>		
<p>Identity Theft: <i>All types of crime in which someone wrongfully obtains another person's personal data in some way that involves fraud or deception.</i></p>	<p>Identity thief, Gary, steals Jamie's social security number and other personal identifying information from her school file. Gary then goes to Target and opens up a credit card in Jamie's name and spends over \$2,000 on a new TV. Gary has committed identity theft because he's impersonating Jamie and opening up credit in her name.</p>	
<p>Identity Fraud: <i>When someone who has obtained another's identity by fraud or deception then uses the identity for a criminal purpose.</i></p>	<p>Kelly steals Angela's driver's license from her purse at lunch. On the way home, Kelly gets pulled over by the police for speeding and reckless driving. Instead of Kelly giving the officer her driver's license, she gives him Angela's driver's license. The ticket is written in Angela's name without her knowledge. Angela finds out someone fraudulently used her driver's license when she gets a ticket in the mail stating she never paid her fees on time. Now she is in bigger trouble with the law.</p>	<p>Troy has a credit card that his parents told him to use for emergencies only. Kevin decides to steal Troy's credit card from his wallet while at gym class to buy clothes after school. Kevin spends over \$250 while impersonating Troy at the store. When Troy realizes that the credit card is missing from his wallet, he tells his parents immediately and they call the credit card company.</p>

[Old School Methods]

Definition	Scenario 1	Scenario 2
<p>Change of Address Forms: A way to secretly divert mail to a criminal's address to gather personal and financial data of a targeted person.</p>	<p>Randy noticed he was no longer receiving his mail. When he went to the post office, they told him his mail had been forward to a new address across town. This new address was unfamiliar to Randy. Thieves have been receiving Randy's mail for the past several weeks.</p>	<p>Rachel posts online that she's excited to leave for her European vacation over the next three weeks. Unbeknownst to Rachel, one of her online friends uses this information to her advantage by filling out a change of address form at the post office. When Rachel returns from her vacation and goes to retrieve her mail from the post office she discovers her mail had been forwarded to an unknown address.</p>
<p>Dumpster Diving: Digging through garbage cans or public dumpsters in search of cancelled checks, credit card and bank statements, or pre-approved credit card offers.</p>	<p>After checking the mail at home, Mike throws out the unimportant pieces without shredding. Come to find out, someone that night went through his trash and found bank account information that Mike had missed.</p>	<p>Susan was working on an important document with many of her client's personal information in it. After her project was complete, she threw the drafts into the garbage instead of placing them in the shredder. Now anyone that has access to the trash has access to the client's personal information.</p>
<p>Mailbox Theft: Stealing mail with personal information from private, curbside mailboxes.</p>	<p>Mrs. Abraham puts her outgoing bills and a birthday card to her niece in the mailbox before school. She puts up the red flag so the postman knows there is outgoing mail. Little did Mrs. Abraham know, her neighbor saw the red flag raised and took all of the outgoing mail without her knowledge. The neighbor now has Mrs. Abraham's check information and birthday gift intended for her niece.</p>	<p>Kyle had his mailbox broken into. There were many pre-approved credit card offers that were sent that day. The thief was able to send in the offers on Kyle's behalf and open new credit cards in his name.</p>
<p>Shoulder Surfing: Secretly watching over someone's shoulder to see what password or other personal information a person types while he or she is online, phone or talking in public.</p>	<p>Max uses the library computer at school every afternoon to check his emails. Melinda decides to sit next to him one day and look over his should while he's typing his password. Melinda now has Max's password and decides to log into his account later that night.</p>	<p>Tia needs to get cash from the ATM for a school trip. While getting money from the ATM there were many people around. Alex saw Tia's PIN number when she typed it in and wrote it down. Later that day, Alex stole Tia's debit card and went to retrieve more cash from the ATM.</p>
<p>Theft: Deliberately stealing a backpack, computer, phone or purse to get access to personal information, or stealing key documents such as a person's driver's license, social security card or birth certificate.</p>	<p>While using the restroom, Trisha's backpack was stolen. Inside were her permission slips, medical information and driver's license for an upcoming trip. Now all of these contents need to be replaced.</p>	<p>Brent's smart phone was stolen from his locker. He didn't have a password on his phone so the thief was able to access all his contacts and information.</p>

FTC-0001252

[Online Dangers]

Definition	Scenario 1	Scenario 2
Internet-Ready Devices: Any device with the capacity to access the internet.	Molly gets a new cell phone for her birthday. She is able check her favorite websites and upload pictures she takes to the internet.	While playing his favorite game, Charlie is able to connect with his friends and people around the world to play against him.
Phishing: An email that looks legitimate redirecting someone to a fake website that will ask for personal information.	Daniel received an email from his school telling him he needed to send in his birth certificate and social security number to an out-of-state address to verify his age. Daniel learned in one of his classes that sometimes fake emails will come through that look legitimate. Daniel showed his dad this email and sure enough, it was fake.	Ella had a credit card for emergencies only. One day she received an email from her credit card company stating her password was about to expire. When she clicked on the link, the bank was asking for a lot of information to “verify” her identity. Ella learned during her computer class that sometimes fake emails will come through that look legitimate. Ella showed her mom this email and sure enough, it was fraudulent.
Social Networking: Connecting with others online through networking sites, blogs and chat rooms and revealing personal information that can be used by criminals to steal your identity.	Taylor set up an online profile to socialize with her friends. She now checks-in to tell everyone where she is, what she’s doing, upload photos, videos and voice memos.	Eddie knows a lot about cooking so he starts a blog journal all of his new recipes, successes and failures in the kitchen.
Spam: Fraudulent emails that promise huge prizes or extreme sales to buy popular items.	Elizabeth signed up from a promotion at the mall with her email address. Over the last week she has gotten many emails from that company and similar companies telling her about prizes and promotions she could win by signing up. Elizabeth knew not to click on these emails or he could possibly get a virus on his computer.	Kirk checked his email one day after school and had 250 new emails from unknown companies and people. Most of the subject lines were offering new TVs for less than \$100. Kirk knew not to click on these emails or he could possibly get a virus on his computer.
Unsecured Wi-Fi Hotspot: Wi-Fi that requires no password to join and can leave you vulnerable when typing in usernames and passwords online.	Ally needs to do her homework online. She also wants to connect to her school’s website, email and messenger. She goes to the coffee shop to connect to their free wireless. A couple days later, Allie’s accounts were hacked into.	Ben decides to download a new app when using the hotel next door’s free wireless. Little did he realize, someone was using free software to screen all username and passwords typed into the unsecured wireless. Ben’s app account has been comprised.

[Cyber Threats]

Definition	Scenario 1	Scenario 2
<p>Badware: Bad software that includes viruses and spyware that steal your personal information, send spam, and commit fraud. Generally, your computer is exposed to badware by downloading an unknown file or attachment.</p>	<p>Samantha needed to buy a program for her science class online. She didn't want to pay for the program so she found a free version on an unknown website. After downloading she found out the "free" software was stealing all of the files off of her computer and publishing them online.</p>	<p>Josh downloaded a file to view X-rated material online. He knew he shouldn't visit this website but since it was free he didn't care. A couple days later, his computer crashed. After getting it fixed, he learned there was a virus he downloaded and was logging all of his keystrokes. Now some thief out there has his usernames and passwords.</p> <p><i>Note: If an identity thief is viewing keystrokes then it means they can see everything you type on the computer.</i></p>
<p>Cyber threats: Threats happening when connected to a device accessing the Internet. (Also referenced as cyberbullying).</p>	<p>Maria goes online to talk to her friends. She starts getting harassed about her outfit she wore to school by a group of girls online. Maria is embarrassed and feels insecure. The cyberbullies were saying some very hurtful things.</p>	<p>Kevin checks his social networking page and he has new posts making fun of his car. The cyberbully even build a website around Kevin and his beat-up car. Kevin is horrified and no longer wants to go to school.</p>
<p>Hacker: Anyone who uses software attack tools to break into computers or smart phones that contain your personal records and steal the data.</p>	<p>Carson sends out a link to his entire class telling them to check out the funny video he made. Carson knew that when his classmates opened the video that it would download a virus to their computer that would give him access to the camera on their computers. Carson wanted to spy on all his friends.</p>	<p>Ashley needed a way to make some extra money for an upcoming vacation so she embedded a virus in her homework project for all her classmates to download. She knew that after her classmate's computers were infected that they would likely log onto their bank accounts and she would have access to them to withdraw money.</p>
<p>Malware: Short for malicious software. Designed to secretly access, damage or disable computer systems without the owner's consent. Generally, your computer is exposed to malware by downloading an unknown file or attachment.</p>	<p>Jose gets an email from someone he didn't know. The email instructs him to download the attached program in order to get faster internet. Once Jose downloads this unknown attachment, his computer crashes and could not be repaired.</p>	<p>Morgan finds a website online that's offering free music and movies. She downloads songs from her favorite artist. After the download was complete she was unable to use her mouse and keyboard. One of the "free" files was infected.</p>

<p>Peer-to-Peer (P2P) File Sharing: Downloading software that allows you to access free music, movies or files that may leave your computer vulnerable for thieves to search the computer for any private documents on the hard drive.</p>	<p>Rex was tired of paying for songs and movies for his tablet. He decides to download software that lets him access free music and movies. Rex didn't know that the free software also opened up his entire hard drive on his device. Everything he had saved could be accessed by anyone with the same software.</p>	<p>Melissa downloaded software that allows her to get free music and movies on her computer. Later that year, her parents complained that someone stole their tax returns and other personal information. Melissa didn't realize that when she downloaded that software, it made it possible for anyone to access their computer's hard drive. Someone from a different state was able to get her parent's tax information.</p>
<p>Spyware: Software that self-installs on a computer, enabling information to be gathered secretly about a person's Internet use, passwords, etc.</p>	<p>Seth disabled his firewall so he could download whatever he wanted without warning pop-ups. Seth found out later that software had been downloaded that was logging all of his keystrokes. All of the websites his parents, siblings and he went to had been logged by a thief. Two days later his parent's had their bank account hacked into.</p> <p><i>Note: If an identity thief is viewing keystrokes then it means they can see everything you type on the computer.</i></p>	<p>Mariah clicked on an ad that popped up about free shoes and it directed her to a fun webpage. What she didn't realize is that the website she went to was accessing her online activity thus compromising her entire computer.</p>
<p>Virus: A program that secretly transmits itself between computers through Wi-Fi or removable storage such as USB drives and CDs. This often causes damage to computers and other users accessing the same devices.</p>	<p>William uses his computer on vacation to go online. He usually connected through unsecured Wi-Fi hotspots to check his email. Now all of his friends are texting him telling him they are getting spam. William thinks it's because he got a virus through the unsecure Wi-Fi.</p>	<p>Monica uses her friend, Sarah's USB device to get Sarah's homework documents for a class project. Once Monica inserts the USB into her computer she notices it's really slow.</p>

[Vulnerabilities]

Definition	Scenario 1	Scenario 2
<p>App: A specialized program downloaded onto your mobile device. In some instances, the app can be fake or your device doesn't detect malicious activity because you've "jail-broken" your phone.</p>	<p>Tia wanted to track her workouts. She went to the app store on her smart phone and downloaded the first one she saw. Once Tia installed the app, it asked her for personal information to track her workouts. Tia didn't know this app was fake and thieves were storing the information she provided to open new accounts.</p>	<p>To track his caloric intake each day, Mark looked into ways to do this on his phone. After reading all of the recommended programs, Mark downloaded the program while at home connected to his secure Wi-Fi.</p>
<p>Cell Phone Camera: Can be used to take a picture or video of any personal information.</p>	<p>Peter and his friends go to the public library after school for homework. While applying for a library card, Peter's friend, Ryan, used his cell phone camera to take pictures of everyone's applications when they weren't looking.</p>	<p>While Lily was changing for PE, Monica was playing with her cell phone in the locker room. Lily found out later when she got online that Monica posted photos of her to a social networking account for everyone to see.</p>
<p>Checks: Checks used to draw money from your bank accounts state your bank account number and routing information, which can easily be copied by a thief who can then fraudulently withdraw from your account.</p>	<p>Christine needed to pay for her new phone but didn't have enough cash on her. She decided to write a check and the funds will be directly taken out of her bank account. A few days later she checked her bank account and more checks were being passed in her name. It turns out that the associate at the phone store took the banking and routing information from the check she used.</p>	<p>When Charlie left for school, his mom gave him a check to pay for his upcoming field trip to the museum.</p>
<p>Credit Card: Plastic card issued by a bank or business designed to make paying for something fast and simple. Purchases are made on credit making it easy for thieves to steal your credit card number if in the wrong hands.</p>	<p>Lucy was given a credit card by her parents to use for emergencies only. After using her credit card online to pay for books, Lucy noticed fraudulent charges. She immediately told her parents and they called the credit card company to close the account.</p>	<p>Troy was looking to build his credit so he applied for a credit card. Now Troy uses his credit card to pay for gas. Each month he pays his bill in full and on time to build up his credit score.</p>
<p>Debit Card: A card issued by a bank allowing the holder to make purchases and the funds are automatically deducted from their bank account making it easy for thieves to have access to your bank account if in the wrong hands.</p>	<p>To learn money management, Tami's parents helped her open a bank account. With her new account, Tami was issued a debit card. Now Tami has to keep track of her PIN number and account balance. Tami told her friend, Cindy, her PIN number so Cindy could buy a snack after school. It turns out Cindy went to the ATM to get money without Tami's consent.</p>	<p>Phil didn't feel safe having his checks in his backpack so he asked his parents for a debit card. Now when Phil needs to make a purchase, he uses his debit card and PIN number to deduct money from his bank account.</p>

FTC-0001256

<p>Location Settings: Features on a smart phone or GPS that allow users to promote where they are located making you a target for online and physical attacks.</p> <p><i>Note: GPS stands for Global Positioning System making it easy to see where you are located.</i></p>	<p>Eva told her parents that she was going to the movies with friends. Instead she went over to her new friend Ben’s house. Her parents showed up 20 minutes later because Eva has apps on her smart phone that show where she is.</p>	<p>Todd uploaded pictures to his blog from the weekend taken with his cell phone. When he posted the photos he didn’t understand how people knew exactly where he was when taking the pictures. Todd didn’t know that the GPS coordinates are recorded in all photos unless deactivated manually.</p>
<p>Skimming: This theft involves a small device called a “skimmer” which is used to copy the stored information in the magnetic strip on the back of your credit or debit card in order to make a counterfeit copy of your card that can then be used or otherwise sold.</p> <p><i>Note: Magnetic strip contains the credit and debit card information that is printed on the card. This is valuable information for identity thieves.</i></p>	<p>When it came time to pay her lunch bill, Sam gave her credit card to the waitress. The waitress left with her card and came back within a few minutes. Later that day, Sam got a call from her credit card company asking if she was buying plane tickets to Maui. Sam told the credit card company she did not make those charges. It turns out the waitress at the restaurant used a skimmer to copy Sam’s credit card. The waitress sold Sam’s credit card number online.</p>	<p>Lindsey paid for gas with her credit card. Days later when she was checking her statement online, she noticed charges that she didn’t make. She immediately called her credit card company and told them of the charges. It turns out there was a skimmer in the gas pump where Lindsey used her credit card.</p>
<p>Smart Phone: Cell phones that have the capacity to go online, store personal data and have many of the same functions as a computer. By losing your device it makes you vulnerable for anyone to have access to that information if not password protected.</p>	<p>Nick has the ability to go online, download music, take pictures and have a GPS through his phone.</p>	<p>Angelina’s phone can track her location so her parents know where she is at all times. Angelina can also go online and upload pictures wherever she is.</p>
<p>Social Security Number (SSN): A nine digit identification number in unique for each individual issued by the Social Security Administration. If in the wrong hands, thieves can open new lines of credit and get a job in your name.</p>	<p>Michael went to the DMV to get his license. He had to provide his SSN in order to verify his identity.</p>	<p>Before Michelle could get her athletic physical, she needed to fill out paperwork at the doctor’s office. The paperwork asked for her SSN so they could verify her insurance coverage.</p>

[Best Practices]

Definition	Scenario 1	Scenario 2
<p>Audience: The potential people who could view anything you post online.</p>	<p>Before Mandy uploaded pictures from her weekend activities she made sure they were appropriate for anyone to see. Mandy’s friend got in trouble a few months ago because the school was checking the student’s social networking pages for bad and illegal behavior, and Mandy did not want to get in trouble</p>	<p>When Sal created his online profile he made sure to use pictures that were professional. If someone saw a photo and post about him that was inappropriate then it could cause him to not get into his college.</p>
<p>Firewall: Designed to block unauthorized access to your device when using the Internet.</p>	<p>Chris got a new computer and part of his package included a firewall and anti-virus protection.</p>	<p>Sophia received her uncle’s old computer for school. Before using it, she took it to the computer shop and had a tune up to check for viruses and update her firewall and anti-virus protection.</p>
<p>Privacy settings: Controls that restrict who can view information on your online profiles. This also pertains to the settings associated with downloads, software, apps or online accounts.</p>	<p>When Cindy gets her new smart phone she views all the settings. She makes sure to turn off the GPS in her camera. She also makes sure the other apps on her phone don’t have the location features activated.</p>	<p>Hank’s parents told him he was able to get a social networking page as long as they could set it up together. Hank and his parents looked at each privacy setting and made sure his profile was private and he wasn’t accidentally sharing his profile, photos and posts with everyone.</p>
<p>Secured Wi-Fi: A wireless technology that allows for an Internet connection from a computer, but many mobile phones, tablets and gaming devices have Wi-Fi as a feature.</p>	<p>Tom decides to grab a smoothie after school. He is supposed to be doing homework so he logs onto his laptop and connects to the internet by using the access card his parents gave him.</p> <p><i>Note: An access card is a secure way to get wireless internet. You’re can buy them through your wireless provider. A unique password is associated with the access card.</i></p>	<p>While Allison is out shopping, she forgets that she needed to pay her cell phone bill. Since there wasn’t a secure place to connect she decides to wait and logon to her account when she’s at home. When she’s at home she connects safely.</p>
<p>Strong Passwords: Using a variety of words, characters, numbers and symbols to protect your online accounts by making them hard to guess.</p>	<p>Angelo has usernames and passwords for many accounts. To increase his safety online, he makes sure his passwords have a combination of upper and lower case letters, numbers and symbols. Angelo always changes his passwords every month and never uses the same password for two different websites.</p>	<p>When Kathy creates her username and password for her school’s homework portal she uses a series of upper and lower case letters, numbers and symbols. She knows if it’s over 10 characters long that it’s harder for her password to be cracked.</p>

Name: _____

Real People, Real Scenarios Student Handout

Identity:	Identity Theft:	Identity Fraud:
Shoulder Surfing:	Theft:	Dumpster Diving:
Mailbox Theft:	Change of Address Forms:	Firewall:
Phishing:	Spam:	Social Networking:

Audience:	Internet Ready Device:	Unsecured Wi-Fi Hotspot:
Cyber Threats:	Virus:	Malware:
Badware:	Spyware:	Peer-to-Peer (P2P) File Sharing:
Hacker:	Smart Phone:	Cell Phone Camera:

Location Settings:	App:	Credit Card:
Debit Card:	Checks:	Skimming:
Social Security Number (SSN):	Secured Wi-Fi:	Strong Passwords:
Privacy Settings:		

Activity 2: The Big Picture (30-40 minutes)

The educator will present a trivia game which summarizes the *Identity Smart: A Guide for Consumers Against Identity Theft* content. The educator can modify the activity to fit the class needs.

Objective:

- Students will play a trivia game which reviews the “Identity Theft” terms and content from *Identity Smart: A Guide for Consumers Against Identity Theft*.

Activity:

Starting the Game

- Your class will be divided into 3 teams.
- Each team will be given a buzzer they will use to answer questions.
- Choose 1 team to pick the first category.

Playing the Game

- Read the question and the first team who buzzes in gets **10 seconds** to answer the question.
- You can work together as a team to answer the question or you can switch off between individual players.
- A correct answer earns the point value while a wrong answer loses the value.
- If the team gets it wrong, the other two teams are given a chance to answer.
- The team who gives the correct answer gets to choose the next category and point value.

Final Round

- At the end of the game, any team with a positive score will play the final round.
- You may wager any point value up to your team’s current score.
- You will have **30 seconds** to write down an answer.
- When time is up, each team will read their answer and award or deduct points based on their wager.
- The team with the highest score wins.

Activity 3: Solutions (20-40 minutes)

The students will play a BINGO game called “ID SMART” which will reinforce the terms while helping students to brainstorm preventative measures which will protect their personal identity information. The educator can modify the activity to fit the class needs.

Objective

- The students will brainstorm proactive measures to help protect their identity information.

Activity

1. Give each student a Handout: ID SMART BINGO.
2. Ask students to fill each square with a term from the Handout: “Identity Theft” terms.
3. Set out the rules of the game:
 - a. The first student to have all the terms in the pattern that the instructor sets, wins.
 - b. These patterns could be: a full row, column, all four corners etc.
4. Randomly call out a term, students should put a check mark in the box if they have written that term on the sheet.
5. The first student to get the required pattern – a full row, column, all four corners and to call out BINGO-- has the opportunity to win.

There is a twist!

6. As the student calls out the terms that helped them to win, he/she cannot win unless he/she can name a preventative measure that will help protect their identity from theft.
7. If students have trouble naming a solution, the instructor can create a list that the students will research (either for homework or on another lab day) or the instructor can provide students with a solution.
8. Send students home with the *Identity Smart: A Guide for Consumers against Identity Theft* booklet and ask them to share it with their parents.


Identity Theft Terms

- **App:** A specialized program downloaded onto your mobile device. In some instances, the app can be fake or your device doesn't detect malicious activity because you've "jail-broken" your phone.
- **Audience:** The potential people who could view anything you post online.
- **Badware:** Bad software that includes viruses and spyware that steal your personal information, send spam, and commit fraud. Generally, your computer is exposed to badware by downloading an unknown file or attachment.
- **Cell Phone Camera:** Can be used to take a picture or video of any personal information.
- **Checks:** Checks used to draw money from your bank accounts state your bank account number and routing information, which can easily be copied by a thief who can then fraudulently withdraw from your account.
- **Credit Card:** Plastic card issued by a bank or business designed to make paying for something fast and simple. Purchases are made on credit making it easy for thieves to steal your credit card number if in the wrong hands.
- **Cyber Threats:** Threats happening when connected to a device accessing the Internet. (Also referenced as cyberbullying).
- **Debit Card:** A card issued by a bank allowing the holder to make purchases and the funds are automatically deducted from their bank account making it easy for thieves to have access to your bank account if in the wrong hands.
- **Dumpster Diving:** Digging through garbage cans or public dumpsters in search of cancelled checks, credit card and bank statements, or pre-approved credit card offers.
- **Firewall:** Designed to block unauthorized access to your device when using the Internet.
- **Hacker:** Anyone who uses software attack tools to break into computers or smart phones that contain your personal records and steal the data.
- **Identity Fraud:** When someone who has obtained another's identity by fraud or deception then uses the identity for a criminal purpose
- **Identity Theft:** All types of crime in which someone wrongfully obtains another person's personal data in some way that involves fraud or deception.
- **Identity:** The collective aspect of the set of characteristics that make you who you are.
- **Internet-Ready Devices:** Any device with the capacity to access the internet.
- **Location Settings:** Features on a smart phone or GPS that allow users to promote where they are located making you a target for online and physical attacks.
- **Mailbox Theft:** Stealing mail with personal information from private, curbside mailboxes.
- **Malware:** Short for malicious software. Designed to secretly access, damage or disable computer systems without the owner's consent. Generally, your computer is exposed to malware by downloading an unknown file or attachment.
- **Peer-to-Peer (P2P) File Sharing:** Downloading software that allows you to access free music, movies or files that may leave your computer vulnerable for thieves to search the computer for any private documents on the hard drive.
- **Phishing:** An email that looks legitimate redirecting someone to a fake website that will ask for personal information.
- **Privacy Settings:** Controls that restrict who can view information on your online profiles. This also pertains to the settings associated with downloads, software, apps or online accounts.
- **Secured Wi-Fi:** A wireless technology that allows for an Internet connection from a computer, but many mobile phones, tablets and gaming devices have Wi-Fi as a feature.
- **Shoulder Surfing:** Secretly watching over someone's shoulder to see what password or other personal information a person types while he or she is online, phone or talking in public.

- **Skimming:** This theft involves a small device called a “skimmer” which is used to copy the stored information in the magnetic strip on the back of your credit or debit card in order to make a counterfeit copy of your card that can then be used or otherwise sold.
- **Smart Phone:** Cell phones that have the capacity to go online, store personal data and have many of the same functions as a computer. By losing your device it makes you vulnerable for anyone to have access to that information if not password protected.
- **Social Networking:** Connecting with others online through networking sites, blogs and chat rooms and revealing personal information that can be used by criminals to steal your identity.
- **Social Security Number (SSN):** A nine digit identification number in unique for each individual issued by the Social Security Administration. If in the wrong hands, thieves can open new lines of credit and get a job in your name.
- **Spam:** Fraudulent emails that promise huge prizes or extreme sales to buy popular items.
- **Spyware:** Software that self-installs on a computer, enabling information to be gathered secretly about a person's Internet use, passwords, etc.
- **Strong Passwords:** Using a variety of words, characters, numbers and symbols to protect your online accounts by making them hard to guess.
- **Theft:** Deliberately stealing a backpack, computer, phone or purse to get access to personal information, or stealing key documents such as a person’s driver’s license, social security card or birth certificate.
- **Unsecured Wi-Fi Hotspot:** Wi-Fi that requires no password to join and can leave you vulnerable when typing in usernames and passwords online.
- **Virus:** A program that secretly transmits itself between computers through Wi-Fi or removable storage such as USB drives and CDs. This often causes damage to computers and other users accessing the same devices.
- **Change of Address Forms:** A way to secretly divert mail to a criminal’s address to gather personal and financial data of a targeted person.

Name: _____

Handout: ID SMART BINGO

I	D	S	M	A	R	T
			<p>Free Spot</p> 			

Become ID SMART

- Write your Identity Theft term in the square.
- Put a check mark in the square when you hear your teacher call that term.
- Think about preventative ways you can protect your Identity Information. Write some ideas here:

**Standards
C3 Matrix**

Common Core Reading, Writing, Listening and Mathematics
ISTE National Educational Technology Standards for Students

C3 Matrix

Cyber-Ethics

Students recognize and practice responsible and appropriate use while accessing, using, collaborating, and creating technology, technology systems, digital media and information technology. Students demonstrate an understanding of current ethical and legal standards, the rights and restrictions that govern technology, technology systems, digital media and information technology within the context of today's society

Cyber-Safety

Students practice safe strategies to protect themselves and promote positive physical and psychological well-being when using technology, technology systems, digital media and information technology including the Internet

Cyber-Security

Students practice secure strategies when using technology, technology systems, digital media and information technology that assure personal protection and help defend network security.

**Common Core English Language Arts & Literacy in History/ Social Studies,
Science, and Technical Subjects Grades 6-12**

**ISTE National Educational Technology
Standards for Students 2007**

College and Career Readiness Anchor Standards for Writing	College and Career Readiness Anchor Standards for Speaking and Listening	Mathematical Practices	2. Communication and Collaboration (a, b)	3. Research and Information Fluency (a,b,c,d)	4. Critical Thinking, Problem Solving, and Decision Making (a,b,c,d)	5. Digital Citizenship (a,b,c,d)
College and Career Readiness Anchor Standards for Reading	College and Career Readiness Anchor Standards for Writing	Research to Build and Present Knowledge (7, 8, 9)	Integration of Knowledge and Ideas (10)	Craft and Structure (6)	Key Ideas and Details (1, 2, 3)	
		Presentation of Knowledge and Ideas (4,5,6)	Make Sense of Problems and persevere in solving them	Construct Viable arguments and critique the reasoning of others	Use appropriate tools strategically	

Identity Smart Educator Resource Guide: Surveys and Materials

Complement to the LifeLock
*Identity Smart: A Guide for Consumers
Against Identity Theft*

Brought to you in partnership with



Brought to you in partnership with:

CyberWatch is an Advanced Technological Education (ATE) Center, headquartered at Prince George's Community College and funded by a grant from the National Science Foundation (NSF). The CyberWatch mission is to increase the quantity and quality of the information assurance (that is, cybersecurity) workforce.

The CyberWatch K12 Division extends the CyberWatch Mission to the K12 Community. Its mission is to advance cybersecurity education by leading collaborative efforts to strengthen the national cybersecurity workforce.

Educational Technology Policy, Research and Outreach (ETPRO), a research and development organization located in Maryland, connects educational technology policy and research to instructional practice. ETPRO brings more than two decades of experience in the educational community, and more than a decade of experience in evaluating both formal and informal educational programs at the K-16 level, and conducting educational technology policy analysis. ETPRO's expertise is founded on a combination of classroom practice across K-16 tied with a solid research base.

ETPRO originated from the Educational Technology Outreach division of the College of Education, at the University of Maryland, and in 2007 was founded as an entrepreneurial entity committed to quality education for all learners, targeting the effective use of cutting edge technology in formal and informal educational settings to increase interest in Science, Technology, Engineering and Mathematics (STEM) fields. The fundamental gap between technology use and understanding of proper practices, lead ETPRO to the forefront of research, program evaluation and development of Cyberethics, Cybersafety, and Cybersecurity (C3[®]) initiatives.

C3 Conference is a high quality professional development event for educators in Maryland and the mid-Atlantic region. The core mission of the C3[®] Conference is to inform the educational community about the ethical, legal, safety, and security implications of technology use and illustrate how educators and parents can apply these concepts to their own setting.

LifeLock, Inc. (NYSE:LOCK) is a leading provider of proactive identity theft protection services for consumers and identity risk assessment and fraud protection services for enterprises. Since 2005, LifeLock has been relentlessly protecting identities by providing consumers with the tools and confidence they need to help protect themselves from identity theft and manage their credit. In October 2012, Javelin Strategy & Research named LifeLock Ultimate™ a "Best in Class Overall" identity theft protection solution and also named it "Best in Detection." In March 2012, LifeLock further demonstrated its commitment to combating identity fraud with the purchase of ID Analytics, Inc., a leader in enterprise identity risk management that provides visibility into identity risk and credit worthiness. ID Analytics, Inc. currently operates as a wholly owned subsidiary of LifeLock, Inc.

Identity Smart Educator Resource Guide: Surveys and Materials

Identity fraud is the fastest-growing category of Federal Trade Commission (FTC) complaints. In 2012, 12.6 million adult Americans fell victim to identity theft.

Federal Trade Commission. "Consumer Sentinel Network Data Book for January – December 2012." February 2013.
Javelin Strategy & Research. "2013 Identity Fraud Report." February 2013

Children make prime targets for identity thieves specifically because they have no credit history and thus, clean credit reports. Also, because parents don't think to check their children's credit histories, the theft can continue unchecked for over a decade. Police agencies are reporting that children are now the fastest growing segment of identity theft victims. Identity thieves will use children's identities to take out loans and lines of credit they never intend to repay and to establish an identity so they can obtain things like jobs or a driver's license.

Unit Overview:

This content is designed to provide educators with the means to explore with students the topic of identity theft and the cyberethics, safety and security strategies associated with it. Students and educators will begin to recognize and internalize the importance of assessing and identifying dangers of identity theft, practicing strategies to minimize the risk and formulating plans and next steps for minimizing the risk of loss in the event of an identity theft.

Objectives:

Upon completion of these lessons and presentations, students will be able to:

- Assess the dangers of identity theft and identity fraud.
- Identify how identity thieves obtain personal information.
- Explain what identity thieves can do with an individual's personal information.
- Practice methods to minimize the risk of identity theft and identity fraud.
- Recognize the warning signs of identity theft and identity fraud.

Materials:

Baseline and Post-Unit Surveys

To begin the content unit on identity theft, you may wish to administer to students the baseline survey. This survey will help you gauge your student's prior knowledge and experiences surrounding the topic of identity theft. A post-unit survey, similar to the baseline survey is also included, and can help you measure changes in student knowledge. Answers keys are provided.

Unit Materials

1. Three baseline and post-unit surveys are included for three different grade bands:
 - Elementary/Early Middle School
 - Middle and High School
 - High School/PTA and Educator Audiences
2. Ice Breaker Scenarios
3. Two case studies, entitled *Security in Cyber Space*,
 - Recommended for use with middle/high school and adult level audiences.
 - The case studies provide an identity theft related vignette that introduces the unit content and helps the attendees to understand why this topic is important.

4. *Parent take home materials* are included and can be used with all age groups.
5. *References* are also included to help access other identity theft stories in the news.

The PowerPoint and case studies can be used separate from or with any of the unit's other activities.

How to Begin:

1. View the materials and the Identity Smart Curriculum PowerPoint.
2. After determining the audience level and format structure, decide on the activities you would like to include. For adults, the open discussion with the PowerPoint is usually enough.
3. The case scenario and PowerPoint is suggested for upper age students. The hands-on activities are suggested for younger audiences.
4. Baseline and follow up surveys are always recommended if time allows.

Ice Breaker Stories (10 minutes)

Activity:

1. Cut each headline and scenario apart and distribute to participants.
2. Divide participants into groups of two or three.
3. Distribute one story to each group. Tell the groups that they are newspaper editors planning to publish the story. Each group is to think of a good headline for their story.
4. Have participants, introduce their group members, and read their headline and story to the entire group.
5. Note: The educator can modify the activity to fit the class needs.

Headline _____

A man and woman in Florida illegally obtained credit card numbers of more than 12,000 patrons of restaurants in Florida and distributed them to others. The couple did this by illegally tapping the computer networks of restaurants, pretending to be a legitimate computer technician servicing the restaurants.

Headline _____

A mentally ill woman exploited a loophole in Washington, D.C. tax office online systems to gain unauthorized access to taxpayer accounts, establish herself as the owner of dozens of businesses and file returns on their behalf. The woman electronically filed FR-500 forms, a document establishing change of ownership or authorized agent, for 114 existing and fictitious businesses. Through the FR-500 process she was able to establish herself as the owner of the businesses and gain access, within 48 hours, to 76 taxpayer business accounts.

Headline _____

The Washington, D.C. Office of the State Superintendent of Education (OSSE) that handles college financial aid requests accidentally e-mailed personal information from 2,400 student applicants to more than 1,000 of those applicants. The OSSE said the breach occurred when an employee of the agency's Higher Education Financial Services Program inadvertently attached an Excel spreadsheet to an e-mail. The information released included student names, e-mail and home addresses, phone and Social Security numbers and dates of birth.

Headline _____

A man had his identity stolen as a child. He found out when his mother filed a tax return with the IRS, when he was 11, for some modeling work that he did. His mother notified the police, the IRS and the Social Security Administration at that time. Several years later she found the illegal alien who was using her son's social security number and the man asked, *Can I keep using your son's social security number? I'll let you have his tax refund.* She told the man to stop using her son's social security number. When the young man went off to college he was denied basic utility services like gas, electricity and telephone service because they said he already had accounts.

Baseline Survey: Elementary/Middle School

Name _____ Date _____

Circle the correct answer

1. This piece of information was given to you at birth by your parents.
 - a. Social Security Number
 - b. Phone Number
 - c. Your Name
 - d. Your high school name

2. This is why people should look around their surroundings when using a computer in a public place and put their hand over the keypad when entering your PIN at the ATM when taking out money.
 - a. Shoulder Surfing
 - b. Skimming
 - c. Dumpster Diving
 - d. Shredder

3. This piece of equipment cuts paper into pieces that make stealing the information on the document difficult to steal.
 - a. Cheese grater
 - b. Skimming
 - c. Jaws
 - d. Shredder

4. These “funny” set of questions sent to you by friends on social networking sites are ways of tricking you into providing identity information about yourself.
 - a. Quizzes
 - b. IQ tests
 - c. Personality tests
 - d. All of the above

5. This method of identity theft is one of the most traditional—and most effective. Thieves search your trash for documents that contain your personal information and gain access to important numbers that help them commit identity theft.
 - a. Stolen wallet
 - b. Dumpster diving
 - c. Phishing
 - d. Shoulder Surfing

6. True or False: Identity theft and fraud is the fastest-growing category of Federal Trade Commission (FTC) complaints.
 - a. True
 - b. False

7. True or False: Since I'm young and don't use the computer or internet as much, I shouldn't be concerned about identity theft?
 - a. True
 - b. False

8. Sometimes thieves pretend to be real businesses and through emails, text messages and what look like real websites, try to get you to give out personal information. These are called...
 - a. Shopping carts
 - b. Dumpster diving
 - c. Phishing scams
 - d. Fake identification

9. There are several protections that you or your parents can do that will keep your computer more secure.
 - a. Update malware protection
 - b. Update the operating system
 - c. Update the web browser
 - d. All the above

10. True or False: You are on the internet and receive a popup announcement stating you could win a free iPhone. This is probably not true.
 - a. True
 - b. False

Post-Unit Survey: Elementary/Middle School

Name _____ Date _____

Circle the correct answer

1. This piece of information was issued to you by the U.S. Social Security Administration.
 - a. Social Security Number
 - b. Phone Number
 - c. Your Name
 - d. Your high school name

2. This is why you should never keep your passwords or social security cards in your wallet or purse.
 - a. Shoulder Surfing
 - b. Stolen wallet or purse
 - c. Dumpster Diving
 - d. Shredder

3. What should you do before you toss out any papers containing personal information?
 - a. Tear up papers
 - b. Crumple up papers
 - c. Shred or burn papers
 - d. Place in the recycling bin

4. These pop up survey quizzes are often forwarded to you by a friend but are really often tricks to get you to share personal information about yourself.
 - a. Answer questions about someone
 - b. IQ tests
 - c. Personality tests
 - d. All of the above

5. This method of identity theft is an old but effective method. Thieves scout for curbside mailboxes and target for theft any mail with identity information.
 - a. Stolen wallet
 - b. Dumpster diving
 - c. Mail theft
 - d. Shoulder Surfing

6. True or False: The number of complaints of identity theft for younger age citizens is growing.
 - a. True
 - b. False

7. Which of the following need to be concerned about identity theft?
 - a. Younger students
 - b. Businessmen
 - c. Grandparents
 - d. All the above

8. A website or text message directs you to go to another website location where you are asked to update your personal information. These are called...
 - a. Shopping carts
 - b. Dumpster diving
 - c. Phishing scams
 - d. Fake identification

9. There are several protection options that you or your parents can do that will keep your computer more secure. Which one(s) can be done to help your computer's security?
 - a. Update your virus protection
 - b. Install operating system and browser updates
 - c. Use spyware detection
 - d. All the above

10. True or False: You are on the internet and receive a popup announcement stating you could win a free iPhone. This is probably a scam.
 - a. True
 - b. False

Baseline Survey: Middle/High

Name _____ Date _____

Circle the correct answer

1. Which of the following is considered to be a safe place to put personal information about yourself?
 - a. Social Networking site
 - b. IM profile
 - c. Webpage
 - d. None of the above

2. This is why people entering password and private information in a smartphone or computer in public should look around, and cover the key pad when entering a PIN number at the ATM:
 - a. Shoulder Surfing
 - b. Skimming
 - c. Dumpster Diving
 - d. Shredder

3. Which of the following are considered to be the next wave of identity theft strategies?
 - a. Malware
 - b. Keystroke logging
 - c. Skimming
 - d. All of the above

4. An email is sent to you indicating that your computer is infected and that you need to download the new antivirus protection to fix the problem. A link to the new program is provided. This is an example of...
 - a. Phishing
 - b. Shoulder Surfing
 - c. Dumpster Diving
 - d. All of the above

5. This method of identity theft is one of the most traditional—and most effective. Thieves search your trash for documents that contain your personal information and gain access to important numbers that help them commit identity theft.
 - a. Stolen wallet
 - b. Dumpster diving
 - c. Phishing
 - d. Shoulder Surfing

6. True or False: Identity theft and fraud is the fastest-growing category of Federal Trade Commission (FTC) complaints.
 - a. True
 - b. False

7. Which of the following will help protect your data and communications when using a computer?
 - a. Password protect your computer and cell phone
 - b. Use strong and diverse passwords/passphrases or patterns
 - c. Avoid logging into private accounts when using free public Wi-Fi (library, coffee shop)
 - d. All the above

8. What program is designed to block unauthorized access to your device when using the internet?
 - a. Malware
 - b. Virus
 - c. Firewall
 - d. Identification Code

9. There are several protections that you or your parents can do that will keep your computer more secure
 - a. Update malware protection
 - b. Make sure when purchasing online you are connected to a secure server (https)
 - c. Update browsers and applications
 - d. All the above

10. True or False: You are on a social networking site and a friend posts a link inviting you to take an online personality quiz. This link could be connected with malware.
 - a. True
 - b. False

Post-Unit: Middle/High

Name _____ Date _____

Circle the correct answer

1. Which of the following is considered to be personal information that should not be posted to your social media site as it could lead to identity theft?
 - a. Full date of birth
 - b. A picture of you
 - c. Names of your friends
 - d. Your high school name

2. The prevalence of cameras and recorders in today's mobile phones make this form of identity theft a real threat. When thieves position themselves within sight or earshot of you as you enter personal information on a smart phone or computer or order merchandise with a credit card over the phone it is called...
 - a. Skimming
 - b. Vishing
 - c. Shoulder Surfing
 - d. Shredder

3. Once installed, malware can run executable programs on your computer without your consent, including transmitting personal information via the Internet to remote computers, where it is stored and sold at a later date to counterfeiters. Which of the following is considered malware?
 - a. Viruses
 - b. Badware
 - c. Spyware
 - d. All of the above

4. A message appears in your social networking site stating, "watch this video of us goofing off." The IP address link is: <http://xh3.8756.986>. This is likely an example of:
 - a. Scareware scam
 - b. Malware link
 - c. Dumpster Diving
 - d. All of the above

5. What can you adjust when you're online to increase your level of security?
 - a. Privacy Settings
 - b. Volume Settings
 - c. Contrast Settings
 - d. All of the above

6. Children are prime victims for identity theft. Youth are now being targeted because:
 - a. They have clean credit reports
 - b. Youth are more likely to share personal data online
 - c. Youth actively use the Internet
 - d. All of the above

7. Which of the following will help protect your data and communications when using a computer?
 - a. Password protect your computer and cell phone
 - b. Use strong and diverse passwords/passphrases or patterns
 - c. Avoid logging into personal accounts when using free public Wi-Fi
 - d. All the above

8. True or False: Music sharing sites and other Peer-to-Peer (P2P) networks give thieves access to any unprotected data on your computer, including personal identity information.
 - a. True
 - b. False

9. There are several protections that you or your parents can do that will keep your computer more secure...
 - a. Update malware protection
 - b. Update your operating system and install patches
 - c. Update browsers and applications
 - d. All the above

10. True or False: Anything stored on the same hard drive as a shared library (P2P) is publicly accessible when you connect.
 - a. True
 - b. False

Baseline Survey: High/Adult

Name _____ Date _____

Circle the correct answer

1. On average, what is the fastest growing sector of the identity theft “industry”?
 - a. Elderly identity theft
 - b. SSN cloning
 - c. Child identity theft
 - d. None of the above

2. Two recent trends related to SSNs and identity theft include criminals increasingly targeting minor’s (even infant’s) SSNs for identity theft, and
 - a. The SSNs of younger US residents are much easier to predict than the SSNs of those born before the 1990s.
 - b. The SSNs of males are targeted more than females
 - c. SSN cloning
 - d. All of the above

3. Which of the following are considered to be the next wave of identity theft strategies?
 - a. Malware
 - b. Keystroke logging
 - c. Spear phishing
 - d. All of the above

4. An email is sent to you indicating that your computer is infected and that you need to download the new antivirus protection to fix the problem. A link to the new program is provided. This is an example of...
 - a. Phishing
 - b. Shoulder Surfing
 - c. Dumpster Diving
 - d. All of the above

5. You can’t entirely remove the risk of identity theft. You can, however, minimize the impact if it does happen. Which of the following steps should be taken as protection measures?
 - a. Stop giving out your or your child’s personal information
 - b. Order a free credit report at least once a year (even if young and haven’t run up credit) or sign up for an identity theft protection service
 - c. If you find evidence of fraudulent activity, contact the police, the source of the fraud and all three credit bureaus.
 - d. All of the above

6. True or False: Personal information posted on a non-private social networking site status update is viewable by anyone online.
 - e. True
 - f. False

7. Which of the following will help protect your data and communications when using a computer?
 - a. Password protect your computer and cell phone
 - b. Use strong and diverse passwords/passphrases or patterns
 - c. Avoid logging into accounts when using free public Wi-Fi
 - d. All the above

8. What program is designed to block unauthorized access to your device when using the internet?
 - a. Malware
 - b. Virus
 - c. Firewall
 - d. Identification Code

9. There are several protections that you can do that will keep your computer more secure . . .
 - a. Update malware protection
 - b. Make sure when purchasing online you are connected to a secure server (https)
 - c. Update browsers and applications
 - d. All the above

10. Suggested password strategies include changing passwords often, using numbers, symbols and upper case letters and which of the following?
 - a. At least 5 characters
 - b. Writing down passwords so you do not forget
 - c. Using a separate password for purchase transactions
 - d. All of the above

Post-Unit Survey: High/Adult

Name _____ Date _____

Circle the correct answer

1. Using an identity theft protection service is one of the best ways to protect your personal information from being misused, but there are also industry best practices you can put in place on your own. Which of the following is considered a recommended best practice?
 - a. Watch your credit score
 - b. Limit the amount of personal data you reveal
 - g. Use strong password tactics
 - h. All of the above

2. Identity theft can take many forms, from stealing your complete profile, to gathering bits of your identity and combining that information with other data to create a fake profile. Which commonly occurs when a thief has stolen your identity?
 - a. A credit card bill is paid in full
 - b. Personal loan paid off
 - c. New service agreements for cellular service or utilities
 - d. All of the above

3. Which of the following are considered to be the next wave of identity theft strategies?
 - a. Pigware
 - b. Cloned debit cards obtained using skimmers
 - c. Mail fraud
 - d. All of the above

4. What can you adjust when you're online to increase your level of security?
 - a. Privacy Settings
 - b. Volume Settings
 - c. Contrast Settings
 - d. All of the above

5. High-risk sources of identity theft include which of the following?
 - a. Emails from friends with no text and just a link to an unknown website
 - b. Peer-to-peer music and movie sharing software
 - c. Logging into your password-protected accounts through free public Wi-Fi sites
 - d. All of the above

6. True or False: Using a search engine to check out an unknown online link provided in an email can uncover if it is fraudulent site.
 - a. True
 - b. False

7. Which of the following will help protect your data and communications when using a computer?
 - a. Password protect your computer and cell phone
 - b. Use strong and diverse passwords/passphrases or patterns
 - c. Avoid logging into accounts when using a public Wi-Fi
 - d. All the above

8. Sometimes thieves pretend to be real businesses and use emails, text messages and what looks like real websites, try to get you to give out personal information. These are called...
 - a. Shopping carts
 - b. Dumpster diving
 - c. Phishing scams
 - d. Fake identification

9. There are several protections that you can do that will keep your computer more secure . . .
 - a. Update malware protection
 - b. Make sure when purchasing online you are connected to a secure server (https)
 - c. Update browsers and applications
 - d. All the above

10. Suggested password strategies include changing passwords often, using a separate password for purchase transactions and which of the following?
 - a. At least 5 characters
 - b. Including numbers and symbols and upper cases
 - c. Changing passwords every two years
 - d. All of the above

Pre/Post-Unit Survey Answers

Question	Elem/Middle		Middle/High		High/Adult	
	Pre	Post	Pre	Post	Pre	Post
1	c	a	d	a	c	d
2	a	b	a	c	a	c
3	d	c	d	d	d	b
4	d	d	a	b	a	a
5	b	c	b	a	d	d
6	a	a	a	d	a	a
7	b	d	d	d	d	d
8	c	c	c	a	c	c
9	d	d	d	d	d	d
10	a	a	a	a	c	b

Case Study 1: Middle/High

Name _____ Date _____

Case Study

Security in Cyber Space

A group of sixth grade girls from Greater City Middle School were meeting at Brianna's house to work on a school project. They had wanted to use some fancy graphics and templates to put a brochure together, so Brianna's mom let them borrow her laptop. They had made a pretty good dent in their project so decided to take a break and check out some social networking pages and funny videos.

Brianna didn't have a social networking account. Her parents told her she could get one on her 16th birthday. "We can use mine," Sarah said. "Your parents let you have one?" asked Brianna. "No, but I really wanted one. So I just set it up myself. I pretended I was older and used another name," Sarah said. Sarah logged into her account. The girls decided to check out some of the eighth grader pages, of the girls they knew from dance class. Nancy was one of the girls from their dance class. "Is she a close friend," Brianna asked. "No, but it doesn't seem to matter. She has it so everyone can see."

Nice dance performance the other night (Sarah), posted Sarah on Nancy's page. "Since I'm showing up as someone else, I placed my name in parenthesis so Nancy would know who it was from," Sarah shared. "Interesting," Brianna said while feeling a little uneasy. "You could do the same thing if you want. Just use my account. Here, I'll write down my password. Just don't post anything stupid," Sarah went on. "Look, someone sent her a link to check out another performance. It says we need to download something else to view it" Sarah exclaimed. Before Brianna could say "No!" Sarah had already clicked and started the download.

Questions for participants to answer.

1. Underline or highlight all questionable practices that you noted in the case study.
2. Of those questionable issues you highlighted in question #1, what consequences could arise?
3. Suggest at least one potential way of addressing each of the issues you listed.

Case Study 2: High/Adult

Name _____ Date _____

Case Study

Security in Cyber Space

Full story can be read at: <http://www.marketwatch.com/story/the-rise-of-identity-theft-one-mans-nightmare-2010-02-10?pagenumber=1>

Identity fraud nightmare: One man's story

Crouse was once an avid fan of online shopping and banking. The Maryland resident with an \$80,000 a year construction-industry job, would auction items on eBay.com, download songs from iMesh.com and often used his debit card like a credit card. While suspicious activity in his account started with small charges of \$37 or \$17.98, charges soon escalated, sometimes adding up to over \$500 per day. Over \$22,000 dollars was charged to his debit card in six months.

He decided to open a new account at a new bank but by the next day the account got hit with a \$1,100 charge. The new bank told him it was keystroke malware that had likely done him in. The thief had hacked into one of the sites he visited regularly, his computer got infected and picked up all his personal information by tracking every key he struck.

Crouse, who has an organizational psychology PhD, had worked previously with both the FBI and Secret Service. When he got laid off from his construction-industry job he thought he would toss his hat back into his previous line of work. While his interviews went well, he kept getting turned down for contract jobs. Finally he learned why. His credit reports were poor and his financial debts were increasing all due to the identity theft. At the time of this story, Crouse was still trying to get out of a mountain of debt and had to take a lower paying job because he lost his security clearance.

Questions for participants to answer.

1. Underline or highlight all questionable practices that you noted in the case study.
2. Suggest strategies to share with others to help reduce the chance of this happening.

Extension Activities 1

Discussion topics:

Do any participants have first-hand knowledge of someone whose personal information was used? If so, have them share.

- Should changes be made in business practices to help stop identity theft? If so, what?
- Are consumers the only victims?
- Are consumers completely responsible for this problem?
- Why do identity thieves steal people's identity?
- What do you think victims feel like after having their identity stolen?
- What are several ways identity thieves can "steal" information?
- For each of the ways listed above, suggest possible solutions.
- What can YOU do to help combat this crime?
- What are some ways a thief could try to trick you into giving him/her your personal data/information?
- Why do you think different studies and surveys, about the number and types of victims, vary so much?
- Share 1-2 things you plan to do to safeguard your identity against theft (or your child's identity).

Projects:

Based on your own experience or someone you know (you may need to interview classmates, an adult or parent), write a paragraph regarding their identity theft experience. When did it happen? What happened? Why did it happen? Did it occur through electronic or non-electronic means? How and when did they realize their identity had been stolen? What type of damage did it cause? What could have prevented it?

- Survey a group of classmates or friends regarding identity theft. You can make up your own quiz from what you learned during this unit or use the parent quiz included in this unit. Or you could also send them to <http://www.sonicwall.com/furl/phishing/> to test their knowledge. Use charts, tables and graphs to share your results. Write a paragraph on your findings.
- Research the history of the Social Security number. What's the purpose? When did it first start? Who got the first card? Whose SSN was most stolen? How is your SSN determined? When are you required to apply for a SSN? Why do some people get a SSN before their first birthday and when was that procedure started.
- Make a list of at least five popular scams and five popular hoaxes and explain them to your classmates.
- Research several surveys or studies on identity theft and explore the impact of this crime at both the individual victim and societal level.

Extension Activities 2

Projects continued:

- Research the most recent malware attacks that have been tied to identity theft. How did they work? Who did they target? Who or how many victims did they effect? What vulnerability was exposed? What would have been possible solutions to counter the malware?
- Create a presentation for your class, another class or PTA group about identity theft and tell them what they need to know about this crime. If possible create a PowerPoint presentation. Start with a few basic statistics and facts to grab their attention. Include the following: assessing the dangers of identity theft, sharing different ways identity thieves obtain personal information, explaining the consequences of identity theft, sharing methods to minimize the risk of identity theft, listing warning signs of identity theft, and plans or next steps to help deter and minimize the loss in the event of an identity theft.
- List 5 to 7 characteristics of a strong password. Make a list of passwords and as a group walk through the characteristics the group created. Will it be easy to guess? Is the password a real word that can be found in the dictionary? Is it at least 8 to 10 characters? Is it a password, passphrase or pass pattern? Does it include upper and lower cases? Numbers and symbols? Will it be easy to remember?
- Research the security of your personal e-mail account. Create a list of e-mail settings. Which of these would you consider to be the most critical? Least critical? Examine your (and/or your child's) personal e-mail settings. How do you measure up? How could you improve your e-mail account settings? Write a short paper or create a presentation sharing your findings.
- Research the differences between identity theft protection services and malware protection services. What can identity theft protection services do besides checking on credit scores?
- Research the types of career options that are associated with the reduction and alleviation of identity theft? Consider Information Technology, secure programming, computer science, Information Systems, forensic sciences, law enforcement, privacy officers and advocates, fraud investigators, digital crime/law and legislators. Why is each important?

Take Home Quiz

Identity thieves use many ways of getting your personal financial information so they can make fraudulent charges or withdrawals from your accounts. Do you know how you can reduce the risk of becoming a victim of identity theft?

Take the simple quiz, and see how you score.

Have your child share what they have learned through their *Identity Smart Unit*. Then take the time to review some of the topics below.

Give yourself 1 point for each item you check off indicating a strategy you take.

Points		
	1	When I keep my ATM cards and credit cards in my wallet or purse, I never write my PIN (Personal Identification Number) on any of my cards or sticky note inside the wallet or purse.
	2	When I leave my house, I take with me only the ATM and credit cards I need for personal or business purchases.
	3	When I get my monthly credit-card bills, I always look carefully at the specific transactions charged to my account before I pay the bill.
	4	When I get my monthly bank statements, credit-card bills, or other documents with personal financial information on them, I always shred them before putting them in the trash.
	5	When I get mail saying I've been preapproved for a credit card, and don't want to accept or activate that card, I always shred the preapproval forms before putting them in the trash.
	6	I request a copy of my credit report at least once a year.
	7	If I think that I may be a victim of identity theft, I would immediately contact the FTC to report the situation and get guidance on how to deal with it.
	8	I regularly update not only my operating system software, but my browser, applications and plug-in software.
	9	I use a separate password for purchasing transactions and all my passwords are changed often, have at least 8 or more characters, and include numbers, symbols and upper and lower cases.
	10	I understand the fastest growing sector of identity theft is <i>child identity theft</i> . Therefore, I have talked to my child about identity theft strategies like limiting the amount of personal information online, and I have checked my child's credit rating.
	TOTAL	

How did you measure up?

Identity Theft Quiz: Answer explanations

1. Reason: If you lose your ATM or credit card, identity thieves or other criminals can have instant access to your bank or credit-card account.
2. Reason: If your wallet or purse is lost or stolen, and you're carrying fewer cards, you'll have to make fewer calls to banks and credit-card companies to report the losses and the odds of fraudulent charges in your name will be lower.
3. Reason: Someone who gets your credit-card number and expiration date doesn't need the actual card to charge purchases to your account. If you don't look closely at your credit-card statement each month, you might not have any recourse if fraudulent transactions go through and you don't dispute them promptly with your credit-card company. As soon as you see unauthorized charges on your statement, contact the credit-card company immediately to report them.

Limit your liability. For credit cards, your limit of liability is only \$50 if you report the fraudulent activity within 60 days. For debit cards, your limit of liability is \$50 if you report the fraudulent activity within 2 business days. If you report between 3-60 days then your limit of liability is \$500. After 60 days the financial institution doesn't have to reimburse you.

4. Reason: Some identity thieves aren't shy about "dumpster diving" - literally climbing into dumpsters or rooting through trash bins to look for identifying information that someone threw out. Buying and using a shredder on your home or office is an inexpensive way to frustrate dumpster divers and protect your personal data.
5. Reason: If you throw out the documents without tearing them up or shredding them, "dumpster divers" can send them back to the credit-card company, pretending to be you but saying that your address has changed. If they can use the account from a new location, you may not know the account's being used in your name.
6. Reason: Any consumer can request one free copy of his or her credit report per year. Reviewing your credit report can help you find out if someone has opened unauthorized financial accounts, or taken out unauthorized loans, in your name. Go to www.annualcreditreport.com to request a copy for you and your children.
7. Reason: Identity theft is a crime under federal law, and under the laws of more than 44 states, that carries serious penalties including imprisonment and fines. To help law enforcement in investigating and prosecuting identity theft, the Federal Trade Commission (FTC) maintains a national database of complaints by identity theft victims. The FTC, through a toll-free hotline (1-877-ID-THEFT), can also help you decide what steps to take in trying to remedy the situation and restore your good name and credit. Credit bureaus should also be notified so that they can flag your credit report. Local police, by taking a report and providing you with a copy, can help you show creditors that an identity thief has been conducting certain transactions in your name and without your permission.

8. Reason: Unpatched software with security holes that have not been plugged place serious vulnerabilities inside your computer, holes that criminals are continually seeking to exploit. Criminals can probe for such vulnerabilities using automated tools that can probe thousands of computers an hour. With a variety of software systems running it's not enough to just update the operating system. Take the time to have updates applied automatically or regularly update software yourself.
9. Reason: Programs to crack passwords or read them from the network are readily available. In order to limit the risk of your password being cracked, it should be at least 10 characters long and include letters (both upper and lower case), digits and symbols. This makes it harder to "crack"—efforts are usually drawn to the lowest hanging fruit. You should change your password regularly and always after a trip where you could have exposed your password at a remote site.
10. Reason: It's difficult to estimate exactly how many children lose their identities since the crime can go undetected for years. Reasons include: (i) a child's identity is a blank slate, and the probability of discovery is low, as the child will not be using it for a long period of time; (ii) parents typically don't monitor their children's identities; and (iii) kids are active online and often give out too much information.

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Services

Our Services

LifeLock Wallet

LifeLock Standard™

LifeLock Advantage™

LifeLock Ultimate Plus™

LifeLock Junior™

Why LifeLock

Choosing the Right Protection

Testimonials

CALL US AT
1-800-607-7205

Send us an email



Secure login



LifeLock Individual Plans: Identity Theft Protection Services

We do more to protect your credit and your good name.

CHOOSE THE RIGHT PROTECTION



LifeLock Standard™ identity theft protection helps keep your personal information safe with the patented LifeLock Identity Alert® system and a whole lot more.†

[Learn more](#)



LifeLock Advantage™ membership adds bank account activity alerts, credit scores and even more protection.†

[Learn more](#)



LifeLock Ultimate Plus™ membership is the most comprehensive identity theft protection ever created.

[Learn more](#)



LifeLock Junior™ is specifically designed to help keep your child's identity information safe.

[Learn more](#)

In today's always-connected world where we all bank, shop, post, email, download and upload, your personal information is everywhere. Your employer has it. Your doctor has it. Anytime you use a computer, go online or use a mobile device, you're at greater risk of identity theft. And, with more and more technology along with an increasing number of data breaches, it's becoming more difficult to keep your personal information safe.

LifeLock provides 3 layers of protection

1. Detect

We monitor over a trillion data points 24/7/365, searching for identity threats to our members.

2. Alert

With the patented LifeLock Identity Alert® system, as soon as we detect a threat to your identity you'll be notified

FTC-0001293

by text, phone or email, to help stop criminals before they do damage to your identity.† **

3. Restore

If your identity is ever compromised, our Certified Resolution Specialists will handle your case every step of the way. And it's all backed by our \$1 Million Total Service Guarantee.‡

LifeLock membership protects you in ways credit monitoring, banks and credit card companies just can't. It's protection beyond what you can provide by yourself. Enrollment takes only minutes and your protection starts immediately.

<p>Identity Theft 101</p> <p>Understanding identity theft and how it can affect you</p>  <p>▶ Learn more</p>	<p>How LifeLock Works</p> <p>See why LifeLock is a leader in Identity Theft Protection.</p>  <p>▶ Learn more</p>	<p>Choose the Right Level of Protection</p> <p>Compare our products and see what's right for you</p>  <p>▶ Learn more</p>
--	--	---

† Network does not cover all transactions

** Fastest alert requires member's current email address.

Most comprehensive protection requires LifeLock Ultimate® membership.

‡ The benefits under the Service Guarantee are provided under a Master Insurance Policy underwritten by State National Insurance Company. As this is only a summary please see the actual policy for applicable terms and restrictions at LifeLock.com/legal.

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

► Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login

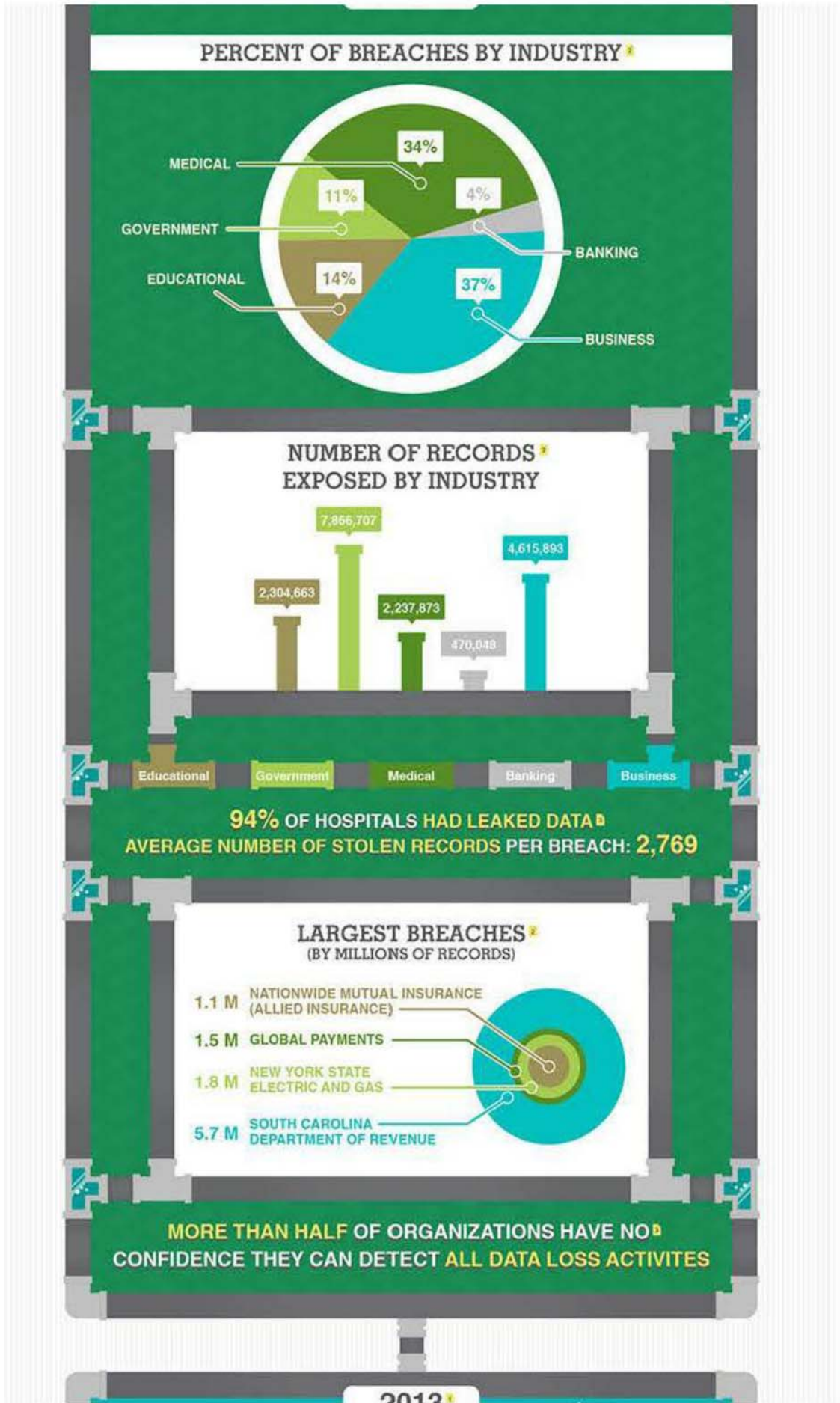


Data Breach Infographic

Share this



FTC-0001295



FTC-0001296

2013

FROM JAN. 1ST TO MAR. 12TH, THERE HAVE BEEN 109 REPORTED DATA BREACHES

PROTECT YOURSELF

- CHANGE YOUR PASSWORD FREQUENTLY
- ENROLL IN IDENTITY THEFT SERVICES
- LIMIT SHARING PERSONAL INFO
- FOLLOW NEWS ON DATA BREACHES



SOURCES:

- [1] <http://www.idtheftcenter.org/>
- [2] <http://www.symantec.com/threatreport/>
- [3] <http://nakedsecurity.sophos.com/2013/01/03/hospital-data-breaches/>



More articles you might like:



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...
As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)



What To Do if Your Company Has a Data Breach
Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Russian Crime Ring Steals Billions of Passwords, O...
A Russian Crime ring has gathered what may be the

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Target Data Breach: What Should You Do?

Share this



:



December 19, 2013

Target today **confirmed that it's investigating the theft of credit and debit card numbers** from millions of customers who shopped at its stores over the past three weeks in what may be one of the largest data breaches ever.

The company says that card numbers, expiration dates and CVV codes -- the three- or four-digit numbers printed on the card to provide extra security -- may have been taken from as many as 40 million people who shopped at U.S. Target stores between November 27 and December 15. People who shopped online or at Canadian Target stores were not affected.

The company hasn't released details, but the United States Secret Service **confirmed to USA TODAY** that it's investigating the Target data breach. All types of cards were affected, including Target's own REDCard credit cards. The company has **posted additional information for customers** and says it's confident that data is no longer being stolen.

Security journalist Brian Krebs has confirmed that **stolen credit and debit card account numbers are appearing on black-market websites** in batches of 1 million cards and selling from \$20 to more than \$100 per card.

If you shopped at Target with a credit or debit card over the past three weeks, there are several things you can do to watch for fraud:

- **Monitor your transactions:** Keep an eye on the activity on your credit and debit cards, looking out for any charges that don't seem to be yours. Rather than wait for a monthly statement in the mail, you can monitor transactions every day using the card issuer's website or a transaction-monitoring tool like **LifeLock Wallet™**.

Related articles

- **New Account Fraud: The Cost of Remediation**
- **Other Types of Identity Theft**

SEE MORE ARTICLES

- **Report suspicious transactions immediately:** If you see something that doesn't look right, contact the card issuer immediately. The phone number is on the back of your card.
- **Watch your credit reports:** You can get a free credit report from each of the three major U.S. credit bureaus each year, and you can pay for more frequent access. Get more information [from the Federal Trade Commission](#).
- **Act fast:** If you believe you're the victim of identity theft, **there are several immediate steps you should take**. If you're a LifeLock member and think you've been a victim, call our Member Services team for assistance at 1-800-LifeLock.
- **Follow the story:** Target and the Secret Service are still investigating this data breach. We'll share more information when it becomes available.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Target Breach Update: What Your Bank Is Saying

Share this



December 24, 2013

Following the announcement that 40 million credit and debit card numbers were stolen from people who shopped at Target stores between November 27 and December 15, some card issuers and customers are now detecting illegal use of those accounts by identity thieves.

In response, many banks and credit card companies are saying that the fraud is being investigated and that customers will not be responsible for fraudulent charges.

Here are links to customer advisories published by some of the larger institutions:

American Express
Bank of America
BarclayCard
BB&T
BBVA Compass
Boeing ECU
Capital One
Chase

Citi
Comerica
FNBO Direct
Commerce Bank
Golden1
Huntington
KeyBank
Navy FCU

PNC
SchoolsFirst FCU
Target REDcard
TCF Bank
USAA
U.S. Bank
Wells Fargo

Learn more about [what you should do in response to the Target breach](#) and read [Target's announcement to customers](#).

Related articles

- [Debit vs. Credit Card ID Theft](#)
- [Target Data Breach: What Should You Do?](#)

[SEE MORE ARTICLES](#)

More articles you might like:

[Tips to Avoid Medicare Card](#)

[Authorities Shut Down](#)

FTC-0001301



Fraud
Seniors just turning 65 may be surprised to find their
[Read story](#)



Suspected Identity Theft Rin...
Whether it's a few people working together on a small-time
[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...
Finding out that you're the victim of a data breach
[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...
As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers
[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

Snapchat Hacked: Were You — Or Your Kids — a Victim?

Share this



Related articles

- How to Pick a Secure Password
- Target Data Breach: What Should You Do?

SEE MORE ARTICLES

January 2, 2014

Usernames and mobile phone numbers for more than 4 million Snapchat users were **apparently stolen from the photo-sharing service this week** by hackers.

If you're a Snapchat user, or if your kids are among the many teens who use it, the good news is that the hackers say they only wanted to call attention to flaws in Snapchat's security. They posted the usernames, along with mobile phone numbers, of 4.6 million users, with Xs in place of the last two digits of each phone number.

A security company that had previously warned of vulnerabilities in Snapchat's security has published **a tool that lets you check the list** to see if your username was exposed.

If your data is on the list, there's nothing you need to do immediately. The biggest danger is that thieves sometimes collect information in small bits and then put it together. For instance, if you or your child use the same username on multiple sites, or if your phone number is available on other sites like LinkedIn or Facebook, someone could potentially match the Snapchat data with what's published elsewhere. You might decide it's safer to use different usernames on different sites, but there's no way to avoid all risks because you almost always have to share at least a little personal information to use any online service.

So the best advice is to remain vigilant about protecting your credit and identity, in case something does happen. If you already have identity protection for yourself, consider also **adding it for your kids**, to protect their busy online lives.

More articles you might like:

CALL US AT
1-800-607-7205

Send us an email



Secure login





Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones
- Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

- Send us an email 
- Secure login 



Scam E-Mail ID Theft

Share this



Related articles

- Fish Out of Water

SEE MORE ARTICLES

Congratulations, you've won!

Did you really win the prize? Does a foreign bank have money for you from an unknown relative? If you're like most people, you have something in your spam folder or an unrecognized email in your inbox right now. Some are from legitimate senders, but others offer the opportunity to buy pharmaceuticals from Canada, notify you of lottery or other winnings, request your help in moving money out of a foreign country or some other supposedly financially advantageous situation. But the unfortunate reality in the majority of these cases is that someone wants to steal your identity.

They say you've won, but in the end you lose.

Spamming has grown along with the growth in social networking. These spams try to get you to click on a link, go to a website and provide sensitive personal information. In many cases, the crooks take some of your money and disappear. But in extreme instances, your bank accounts are emptied and your available credit used up.

Typical scam emails attempting identity theft involve representing a financial institution, retailer or other trusted entity attempting to you sell you goods or services, or asking you to update or provide financial information for your account.

But how do you know?

When reviewing a questionable email, one of the first things to look for is incorrect spelling or bad grammar. Many phishing emails are poorly written or have frequently misspelled words. Also, look for links within the email, and don't click on them. If you place your mouse over the link and view the address, you may find it does not match the party that the email is purportedly from. If the language in the email is threatening, alarmist, requires you to do something immediately or promises you money with little or no effort on your part, think again. Most banks and other legitimate businesses and organizations do not send emails requesting important personal information.

Make common sense more common.

If you receive an email from a financial institution or company you have an account with, and it requests urgent action, simply place a call to the company using a number on a statement or card to see if it is a valid request. If you receive notice of a package containing money, or that you've won a lottery or are asked to accept a foreign funds transfer, realize that no money would need to be paid nor any sensitive information required if it were legitimate.

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Mobile Wallet

Share this



:



Related articles

- Smartphone Data Theft

SEE MORE ARTICLES

A Mobile Wallet will need to be secured differently.

With all the new smartphones being launched this year, you're probably hearing a lot more about terms such as Mobile Wallet and Near Field Communications (NFC). Sooner or later (bet on sooner) they're sure to impact you directly.

The Mobile Wallet may eventually replace the contents of your oh so cool imported leather wallet. Instead, everything will be digitized and stored in your smartphone—credit cards, banking information, retail store cards, coupons, boarding passes, loyalty cards, movie tickets. Want to make a purchase? Just wave your phone and get on your way.

Here are the three current approaches you've probably heard the most about:

1. Google Wallet. Allows you to store credit and debit cards on your Android phone and just tap the back of your phone on an NFC terminal at the point of sale. (More about NFC later.)
2. Apple Passbook. Apple users with iOS6 devices can create a virtual wallet to hold their movie or sporting event tickets, store membership cards, boarding passes, hotel confirmations and more.
3. Windows 8 phone users will also have NFC capability and tap-to-pay.

What is NFC?

Near field communications is technology that allows close-proximity two-way communication between a mobile device and an NFC enabled payment terminal. Actual field implementation is still limited but mobile commerce is expected to increase over time.

How is all this connected to security and identity fraud?

The more personal information you have on your phone, the more secure it should be. According to the February 2012 Identity Fraud Survey Report by Javelin Strategy & Research, smartphone users are 35% more likely to experience fraud than the average consumer. That's huge. And if you're already 35% more likely to experience fraud because of your smartphone, what happens when you store even more financial information on it?

Begin with these steps to make your smartphone more secure.

- ▶ Create an access password for your phone
- ▶ Log out of open apps
- ▶ Be careful about downloading free apps from app stores you're not familiar with, they could contain malware
- ▶ Don't post personal information on social sites
- ▶ Monitor your credit card use and promptly check your statements

A mobile wallet may become a real convenience for you, but take some extra precautions so it isn't equally convenient for an identity thief.

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Why Teens Are at Risk for Identity Theft
Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook
Check your Facebook timeline. Chances are that with very little [Read story](#)



What is Caller ID Spoofing?
Your phone number plays a prominent role in identifying you [Read story](#)



Phone and Utilities Fraud
Service agreements for cellular service or utilities are common means [Read story](#)

Displaying 4 of 7 Results. [Show More Results](#) ▶





Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Donating Your Tech Gadgets? Wipe Them First



Share this



Related articles

- [Cellphone Security: What to Do to Keep Teens Safe](#)
- [How to Avoid Identity Theft at Wi-Fi Hotspots](#)

SEE MORE ARTICLES

Did you get a new smartphone or laptop over the holidays?

Technology moves fast, and for most of us, that means we have a pile of old, unused and obsolete gadgets sitting in a drawer, our basement, attic or garage.

These days, many charities are accepting old computers, smartphones and other devices, and this is a great way to both help those in need and clean out your leftovers.

Before you donate or recycle your phone, computer or any other device where your personal information may be stored, here are some tips to make sure you don't donate your identity along with it.

Thrift stores, flea markets and even eBay are prime sources for identity thieves, [PC World reports](#), and the thieves literally bank on the fact that most folks don't take time to erase data before donating or selling.

Here's how to remove your data—completely—before giving your gadgets away.

For Hard Drives: Wipe

Reformatting a hard drive or moving files to the recycle bin makes the information unsearchable, but does not actually delete it or prevent content from being retrieved by a data recovery tool, says Patrick Miller, a technology expert and [PC World](#) columnist.

For completely cleaned technology, [Geek Squad](#) recommends [DBAN](#) to remove your information permanently. With the creation of a bootable file and just a few keystrokes, DBAN will begin blowing your data away.

For Phones: Restore Factory Settings

An article from [FoxNews.com](#) details the types of personally embarrassing and damaging information that people leave on their cellular devices before giving them away.

Embarrassing is one thing. (An iPhone bought on Craigslist reportedly still had a text from its user admitting, "I'm talking about dressing up like a woman for Black Friday [for the] sympathy.") But ID thieves armed with so-called forensic technology are also able to dig up Social Security and credit card numbers, user names and passwords.

Two forensics technology experts—Andrew Hoog, chief investigative officer at viaForensics, and Lee Reiber, director of mobile forensics for AccessData—offered smart tips to FoxNews.com to wipe sensitive data from your devices before you donate them.

1. Restore the device's factory settings. There should be a "reset" option in the settings applications.
2. Remove your Subscriber Identity Module (SIM) and Secure Digital (SD) cards. Data is stored there.
3. Run updates on the phone's operating system to wipe out a large portion of the data found in the phone's file system.

Be sure to read your owner's manual and back up your data safely and securely before erasing anything.

Apple Products

According to Apple, you can delete settings and information from your iPhone, iPad, or iPod touch using "Erase All Content and Settings" in Settings > General > Reset.

This could take a while, so make sure your device has a full charge before beginning. If there is not a full charge, connect it to power until the process is finished.

For Mac computers, [Macworld advises](#) to start Disk Utility in the Utilities folder, and choose the drive you'd like to erase from the left side of the window. Click Erase and then Security Options—there will be four choices ranging from the least secure option (Don't Erase Data) to the most secure (35-Pass Erase).

Buyer Beware, Too

If you buy a used device, take precautions. "You need to go through the steps like it's yours to get rid of that data," Reiber told FoxNews.com. Something criminal left on the device could prove incriminating for the new owner, he said.

So if your new phone still has the previous owner's data, delete it right away.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach



Identity Thieves Target Outgoing Mail

Police in Chesterfield,

FTC-0001311

Big data breaches at stores like Target, Neiman Marcus and [Read story](#)

Missouri are warning residents that leaving outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Children Often Victims of Identity Theft

By Marcia Simmons
May 13, 2014

Share this



Adults aren't the only ones who have to worry about having their identities stolen.

Each year between 500,000 and 750,000 children living in the United States are affected by identity theft, according to law enforcement professional and former fraud supervisor Robert Chappell Jr., author of "[Child Identity Theft: What Every Parent Needs to Know](#)."

Out of all consumer complaints reported to the FTC in 2013, 6 percent of the victims were children.

And a [study by Carnegie Mellon's Cylab](#) in 2009-2010 provided "some disturbing evidence that identity thieves are targeting children due to the unique value of unused Social Security numbers."

A child's identity is a blank slate for thieves — unused Social Security numbers can be paired with any name and birth date for fake IDs and there's little chance of discovery since most parents don't monitor their children's identities.

The Saffell family of Tulsa, Okl. didn't know their 3-year-old son's identity had been stolen until the IRS denied their tax return this year because someone else had already claimed him as a dependent, [Fox23 News reports](#). They are still unable to claim him, which means they now owe the IRS money rather than receiving a return and must wait until the investigations pan out to recoup.

"Because of privacy laws we're not allowed to know the name of the person who stole our son's identity, which I think is ridiculous. Where were the privacy laws when they took my 3-year-old's Social Security number?" Violet Saffell told Fox23.

More commonly identity thieves will use a child's Social Security number to open new accounts, which may
FTC-0001313

Related articles

- [School Data Breaches Leave Young Children Vulnerab...](#)
- [States Struggle to Make Birth and Death Certificat...](#)
- [When Identity Theft Hits Home](#)

SEE MORE ARTICLES

not come to light until the child is older and tries to rent an apartment or get a credit card. The Cylab study of about 40,000 children found 537 whose identities were tied to mortgages or foreclosures. The youngest victim in the study was 5 months old.

Stephanie McManis is 31 years old, yet she still receives collections calls and lawsuit threats about accounts opened under her name by identity thieves when she was only 12 years old, [according to the Huffington Post](#).

There are many other stories like McManis's, whether the result of [someone hacking a school district's computers](#) or the [child's own family members violating their trust](#). In [Florida](#), the nation's hotspot for identity theft of any stripe, about 50,000 kids a year are victims of identity theft to the tune of \$100 million annually, the [Orlando Sentinel reports](#).

To help combat this problem, many states are drafting legislation to protect children from ID thieves. A new bill in Florida similar to an [existing Wisconsin law](#) proposes that parents and guardians would be able to open a file with one of the major credit bureau's in their child's name and then put a lock on it to keep potential fraud at bay.

Such laws are on the books already in Delaware, Oregon and Maryland with Texas and Illinois also considering similar laws. There's a [national law](#) already in place that requires credit checks on older foster children and offers help in resolving credit disputes and identity theft problems, since foster children are particularly vulnerable to this kind of violation.

Experts agree parents need to vigilantly guard their children's personal information and recommend monitoring their identities as well. Unfortunately, children who've had their identities stolen by their parents may be left to sort through these problems later as adults.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Foster Kids Face Heightened Risk of Identity Theft

By Drew Himmelstein
June 03, 2014

Share this



Every year, **26,000 children age out of the foster care system**, usually when they turn 18, according to the Federal Trade Commission. Many of them are on their own to take the steps needed to set up adult lives: renting apartments, getting cell phone plans and enrolling in college.

And every year, many foster kids learn for the first time that they are victims of identity theft and will be held back in establishing their independence by years of accumulated bad credit in their names.

"It's a really difficult crime to monitor," according to Nikki Junker with the Identity Theft Resource Center. "You know that they are more vulnerable simply by their information being passed around."

When a child is in foster care, his personal documents are passed between family members, caseworkers, foster homes and other providers. There is a heightened risk for loss and abuse of this sensitive information.

That's why Congress passed a law in 2011 requiring child welfare agencies to get annual credit reports for foster children starting when they're 16 and help them clear up any inaccurate information. The U.S. Department of Health and Human Services estimates there are 74,000 foster children in the U.S. age 16 and older.

Children under the age of 18 aren't even supposed to have credit reports — in most cases, they're too young to get credit cards or enter into other contracts. But all too often, the credit reports — with erroneous and fraudulent histories — are there.

Related articles

- Being Smart When Kids Return to School
- Children Often Victims of Identity Theft
- School Data Breaches Leave Young Children Vulnerab...
- Youth at Risk

SEE MORE ARTICLES

"We know it's an issue nationwide," said Karen Barney with the Identity Theft Resource Center. "It totally wrecks your credit, especially when it comes to getting into college.

A 2013 [report by the Annie E. Casey Foundation](#) estimated that 5 percent of foster children aged 16 and older have some form of bad credit.

Recently, the Consumer Financial Protection Bureau [published template letters](#) that caseworkers can send to credit bureaus to report errors in foster children's credit reports.

"The Bureau is very concerned about foster care children's vulnerability to credit reporting problems that can wreak financial havoc for them," said Richard Cordray, director of the Consumer Financial Protection Bureau, in a statement. "We want to help ensure that youth leave foster care with clean credit so that they have a firm foundation for their financial future."

Bad credit can make it difficult for former foster children to rent an apartment, get student loans, get a job and buy a car, according to the Annie E. Casey report.

The new tools released by the Consumer Financial Protection Bureau include letters caseworkers can send credit agencies to notify them that a credit report wrongly exists for a minor or that there is an error in a foster child's credit report.

The Consumer Financial Protection Bureau also recommends that foster care caseworkers educate children on the importance of good credit and how to maintain it.

Drew Himmelstein is a writer and digital storyteller based in San Francisco. Her work has appeared in the San Francisco Chronicle, Dwell Magazine, American Craft and on NPR, and she is a former editor at Patch.com. She holds a master's degree in journalism from University of California, Berkeley.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Identity Theft Remains the Top U.S. Consumer Complaint

By Jamie White
February 27, 2014

Share this



Identity theft continues to top the list of consumer complaints, and when it's combined with other kinds of fraud, the total losses reported by U.S. consumers totaled more than \$1.6 billion in 2013, according to a Federal Trade Commission report released Thursday.

Florida had the highest per capita rate of reported identity theft complaints, followed by Georgia and California. Nearly 300,000, or 14 percent of the 2 million complaints the FTC received last year, were related to identity theft, [the report](#) said.

The majority of identity theft grievances were related to taxes or wages.

Government documents and benefits fraud — the most common category — accounted for 34 percent of identity theft reports.

Credit card fraud comprised 17 percent of complaints, followed by phone or utilities fraud at 14 percent and bank fraud at 8 percent.

The highest reported age group for identity theft is 20-29, making up 20 percent of complaints, but the FTC warns that anyone can be a victim.

"Americans of all ages are vulnerable to identity theft, and it remains the most common consumer complaint to the Commission," Bureau of Consumer Protection Director Jessica Rich said in a statement. "We urge consumers to visit FTC.gov/idtheft for tips to prevent and mitigate the damage from identity theft."

More than 1 million complaints reported to the FTC last year were related to fraud, with half the victims noting that scam artists first contacted them by phone or email.

The Federal Trade Commission advises anyone who spots a scam, is the victim of identity theft or other fraud-related issues to file a complaint online with the agency's [Complaint Assistant](#) or call 1-877-FTC-HELP (877-382-4357).

For more information on tax-related identity theft, click [here](#) and [here](#).

For information on protecting your identity, click [here](#).

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001320

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Eye Scanner Could Make Passwords Obsolete

By Jamie White
January 22, 2014

Share this



Related articles

- How to Pick a Secure Password
- How to Protect Your Identity

SEE MORE ARTICLES

If one of your New Year's resolutions is to secure your identity and digital footprint, there's one company to keep your "eye" on this year.

As simple as looking into a mirror, **Eyelock's** Myris technology controls access to your computer and secured websites. If you're willing to shell out \$300, you could soon be free of usernames and passwords.

The **Myris device**, which is the size of a computer mouse, was presented at this month's **Consumer Electronics Show** in Las Vegas.

Myris will work with Windows 7 and 8, Mac OS and Chrome OS when it becomes available later this year. You'll plug it into a USB port and use its application to authenticate your identity through the irises of your eyes. The company offers a **video** that demonstrates how it works.

Since no two irises are alike, the company says the chances of a false match are less than 1 in 1.5 million -- or 1 in 2 trillion when it checks both of your eyes. With fingerprint recognition being used in devices like the iPhone 5S, the company says the chances of a false positive are 1 in 10,000.

"EyeLock is the first company to employ a unique iris authentication process that leverages video based dual-eye authentication," said Eyelock Chief Marketing Officer Tony Antonino. "This process identifies more than 240 points of unique characteristics in each human iris."

Myris will be available in the first half of this year for less than \$300, Antonino said.

FTC-0001321

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)



What To Do if Your Company Has a Data Breach

Big data breaches at stores like Target, Neiman Marcus

and [Read story](#)



Identity Thieves Target Outgoing Mail

Police in Chesterfield, Missouri are warning residents that leaving

outgoing [Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



FTC-0001322

Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



How to Avoid Identity Theft at Wi-Fi Hotspots

Share this



Related articles

- Top 10 Tips for Safe Online Shopping

[SEE MORE ARTICLES](#)

While you're taking care of business on your laptop at the neighborhood coffeehouse, there may be a person across the room — or in his car across the street — busy on his laptop or smartphone, too.

Except that he's busy capturing what he needs over the public Wi-Fi airwaves to steal your identity, drain your bank account or max out your credit card. That may be the priciest latte you ever ordered.

Before You Go

1. Strengthen your security. Be sure your laptop security is up to date, says the FBI, with current versions of your operating system, Web browser, firewalls and anti-spyware software. This is good advice even when you're working at home, just in case that neighbor who never says much is up to no good. But at a coffeehouse or airport where you're surrounded by strangers with laptops, it's crucial.

2. Protect your passwords. You know how websites and browsers ask if you'd like them to "remember" (save and store) your password? Just say no, according to *PC Magazine*. "You're probably better off not storing your username and password anywhere and that goes double for road warriors who frequently connect via public Wi-Fi," the magazine says. Storing this data on an encrypted passport management application is probably safe, however.

3. Pick your spots. Some wireless hotspots are very safe to use, while others have no security safeguards at all. If you have a choice, such as two coffeehouses on the same block, choose the one that requires online registration with a log-in password. The most secure networks require a password for access because they're encrypted; avoid "unsecured" networks that let you in with no password required (they may be planted by a nearby hacker), says *PC Magazine*.

Going Online

4. Turn it off. Don't forget to turn off (disable) File Sharing, and remove any files that might be in your Shared Documents or Public folder, according to About.com's mobile office technology expert, Melanie

FTC-0001323

Pinola. Also, disable your ad-hoc wireless network if you use an intranet network through your employer.

5. Select the right network. When you choose among Wi-Fi networks, *manually* select one after changing the default setting (if necessary) on your laptop, says the FBI. Choose "Public" or "Public Network" if your computer gives you that option. (Public Network locations block file and printer sharing from potential data thieves.) Of course, be sure you connect to a known network, not just the one with the most bars.

6. Use a VPN. If you don't already use a Virtual Private Network (VPN) during Wi-Fi sessions on your home or work computer, consider it now. According to *PC Magazine*, VPNs keep your data and communications in a "virtual tunnel ... secured against anyone who may try to intercept your Web session while connected to a public hotspot."

Playing It Safe

7. Surf with care. Avoid financial transactions like online banking and e-commerce. If you can, also limit or avoid instant messaging and checking Web-based email because they may not be encrypted. In general, don't go to sites that may not be secure (secure sites begin with "https") or that may reveal sensitive information. Wait until you get home.

8. Watch your back. Even if you take all of these steps, don't forget about "brick-and-mortar" theft. Some identity thieves "shoulder surf" in crowded places: sitting beside or behind you while hoping you'll type your credit-card number or a key password. Change tables if you're suspicious. Or they may simply snatch your laptop.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶





Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



ID Theft Ringleaders Face Stiff Sentences

By Marcia Simmons
March 19, 2014

Share this



Several people involved in identity theft rings were recently sentenced, while another two men face more than three decades in prison if convicted of stealing the identities of 4,200 victims.

ID Theft Mastermind Sentenced for Duping Retailers

William Dodge was sentenced to seven years in federal prison for leading an identity theft ring that cost retailers almost \$400,000, [according to the Federal Bureau of Investigation](#). The judge also ordered the 46-year-old Massachusetts man to pay restitution to the retailers for the full amount stolen.

Dodge's girlfriend worked in human resources at a Florida-based company and he paid her \$3,000 to give him her co-workers' personal information, the [Salem News reports](#). Along with at least five co-conspirators in 30 states, Dodge used these stolen identities to get fake drivers' licenses.

The accomplices or Dodge himself would pose as customers who'd lost their store credit card. They'd then ask the cashier to look up the account using the phony drivers licenses. If the person whose identity they were using had a credit card with the store, a member of Dodge's crew would charge items to the account. If not, they would later open an account under the stolen identity using their fake ID.

They would purchase gift cards or merchandise they could resell. As ringleader, Dodge took 50 percent of the other members' profits. Overall, the group netted more than \$375,000 in merchandise and services, with Dodge personally responsible for more than \$212,000 of the losses.

Retailers affected include J.C. Penney, Best Buy, The Home Depot, Lowe's, Kohl's, Macy's and T.J. Maxx.

Ringleader Gets 12 Years for Stealing Government Employee Identities

The head of a ring that used hundreds of stolen government employee identities to steal almost \$2.5 million was sentenced to 12 years in prison, [UPI reports](#).

Jenaro Blalock, who pleaded guilty last year to stealing at least 600 identities, was also ordered to repay more than \$1 million in restitution.

Between June 2011 and July 2013, Blalock and co-ringleader Christopher Bush recruited women with access to employee data from the State Department, the Pentagon and the U.S. Agency for International Development to hand over identity information from their employers.

Blalock, 31, and his theft ring then used the information to make fake driver's licenses, get retail credit

cards and rent cars and then sell them on the black market with altered vehicle identification numbers.

Bush was sentenced in January to 10 years in prison for his role in the scams.

Tijuana-Based ID Theft Ring Indicted for Hacking Mortgage Broker Servers

Two men were indicted for their suspected role in a Tijuana-based conspiracy that hacked computer servers of a U.S. mortgage broker to steal customer information and siphon funds from thousands of customer accounts, [according to the Federal Bureau of Investigation](#).

California residents Jason Ray Bailey and Victor Alejandro Fernandez were charged with conspiracy to commit wire fraud and computer hacking. Authorities say the men impersonated the mortgage broker's customers, and then used their stolen personal information to open credit lines in their names and take their assets.

After gaining control of the accounts, Bailey and Fernandez allegedly wired funds from the victims' brokerage accounts to U.S. bank accounts in the San Diego and Calexico areas. Some of these wires were for more than \$20,000 and \$30,000 each.

About 4,200 customers had their information stolen between December 2012 and June 2013, and the conspiracy dates back to July 2011.

Bailey and Fernandez, both 38, pleaded not guilty and are scheduled for a motion hearing and trial setting conference on April 11.

If convicted, both men face up to 35 years in prison and a fine of \$1.25 million in the case.

Marcia Simmons is a freelance writer living in the San Francisco Bay Area. Her work has appeared in Every Day with Rachael Ray, Shape, Go, Geek, among other publications. She has also served as managing editor for the North Bay Business Journal and an editor for the Project Censored series of books.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Ring...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results.. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-
7205

Send us an email



Secure login



Phone Scam: U.S. Warns of Calls from Fake IRS Agents

By Jamie White
March 27, 2014

Share this



Taxpayers should be on high alert for identity thieves pretending to be from the IRS, the U.S. Treasury warns.

More than 20,000 taxpayers have been targeted, including thousands of victims who have paid over \$1 million to criminals claiming to be IRS officials, said J. Russell George, the Treasury Inspector General for tax administration, in a [news release](#).

"This is the largest scam of its kind that we have ever seen," George said.

The fraudsters tell people they owe taxes and must pay with a prepaid debit card or wire transfer. They threaten those who refuse to pay by telling them they will be arrested, deported or lose a business or driver's license if they don't pony up the money.

George said the phone scam has affected victims in nearly every state.

The IRS usually contacts people by mail – not by phone – about unpaid taxes and won't ask for payment using a prepaid card or wire transfer, George said. The IRS also won't ask for a credit card number over the phone.

"If someone unexpectedly calls claiming to be from the IRS and uses threatening language if you don't pay immediately, that is a sign that it really isn't the IRS calling," he said.

The callers who commit this fraud often:

- ▶ Use common names and fake IRS badge numbers.
- ▶ Know the last four digits of the victim's Social Security Number.
- ▶ Use fake Caller ID information appear as if the IRS is calling.
- ▶ Send bogus IRS e-mails to support their scam.
- ▶ Call a second time claiming to be the police or department of motor vehicles, again with fake Caller ID.

If you get a call from someone claiming to be with the IRS asking for a payment, here's what to do:

- ▶ If you owe Federal taxes, or think you might owe taxes, hang up and call the IRS at 800-829-1040.
- ▶ If you don't owe taxes, call and report the incident to the Treasury Department at 800-366-4484.
- ▶ You can also file a complaint with the Federal Trade Commission. Add "IRS Telephone Scam" to the comments in your complaint.

FTC-0001329

The IRS offers more information about various kinds of tax scams [on its website](#).

Jamie White is the managing editor of news content for LifeLock. As a journalist for the last 15 years, she has worked as a reporter and editor at news organizations throughout the San Francisco Bay Area, including The San Francisco Examiner. Most recently, she was a regional editor for Patch Media, a local news and information consortium of 900 websites nationwide. Jamie holds a master's degree from Columbia University's Graduate School of Journalism.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results.. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms. & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



Cellphone Security: What to Do to Keep Teens Safe

Share this



Related articles

- Smartphone Data Theft

SEE MORE ARTICLES

Remember the old days when parents used to complain that their kids spent too much time on the family phone with their friends? Well, now we just wish our kids would talk. According to a recent study by The Pew Internet & American Life Project, 23 percent of U.S. teens now own smartphones and a majority (63 percent) are using them to text friends instead of call them—to the tune of 3,339 text messages a month on average.

But that, Mom and Dad, shouldn't be your biggest concern. Just having a smartphone makes your kids an easy target of cybercriminals. Hackers are targeting smartphones because they're a treasure trove of personal data. In 2011, 7 percent of smartphone owners were subject to identity fraud, according to a report by Javelin Strategy & Research—a frightening number when you consider that almost 25 percent of kids ages 12 to 17 have a smartphone, as reported by Pew Research Center.

Here are six cellphone security tips that can protect your child and his or her phone.

- 1. Set the screen lock.** For an iPhone, you can choose a four-digit numeric PIN or an eight-character alphanumeric passcode, which is more secure. For an Android phone, screen locks vary by device. You can also set the phone to auto-lock after a preselected time delay so your child doesn't have to keep reentering it.
- 2. Choose a tricky passcode.** Avoid obvious passcodes like 1111, birthdays, addresses and the like.
- 3. Activate auto-delete.** This cellphone security feature should be turned on to wipe out data in case the phone is lost or stolen. You can set it to wipe all the data after a specified number of failed attempts to get into the phone.
- 4. Turn off Bluetooth, Wi-Fi and GPS when not in use.** Hackers can tap into phones using these programs.
- 5. Get the updates.** Operating system updates usually include cellphone security patches, so install them right away.

FTC-0001331

6. Download applications only from reputable sites. The iPhone apps are vetted by Apple and usually secure, but Android apps can come from anywhere—including cybercriminals. Be sure to read the permissions list and see what you might be agreeing to.

Sources:

<http://www.pcmag.com/article2/0,2817,2403389,00.asp>

<http://ezinearticles.com/?9-Must-Do-Practices-for-Smartphone-Security&id=6407246>

<http://www.itworld.com/hardware/185707/how-prevent-your-smartphone-being-hacked>

<http://blogs.wttw.com/moreonthestory/2011/07/19/cell-phone-hacking-prevention-tips/>

More articles you might like:



Why Teens Are at Risk for Identity Theft
Identity theft is more common among kids, teens and college [Read story](#)



5 Steps to Protect Your Identity on Facebook
Check your Facebook timeline. Chances are that with very little [Read story](#)



What is Caller ID Spoofing?
Your phone number plays a prominent role in identifying you [Read story](#)



Phone and Utilities Fraud
Service agreements for cellular service or utilities are common means [Read story](#)

Displaying 4 of 7 Results. [Show More Results](#) ▶



Identity Theft 101

Identity Theft News

- Alerts
- Crimes
- Data Breaches

Identity Theft Protection

- Basics
- Children/Family/Home
- Computers and Technology
- Smartphones
- Your Money and Finances

Identity Theft Recovery

- Basic Steps
- Credit Score Help
- Lost and Stolen Items

Understanding Identity Theft

- Electronic Communication
- Fraud
- Social Networks

CALL US AT
1-800-607-7205

Send us an email 

Secure login 

Skimming Devices



Share this



Related articles

- Internet Privacy and ID Theft Protection

SEE MORE ARTICLES

Skimming, whether on a handheld device or on a point-of-sale device (like a credit card machine at the checkout line), involves the theft of your credit or debit card information while being used during an otherwise legitimate purchase or transaction.

How Does ATM/Handheld Skimmers Theft Occur?

Skimmers are small electronic devices that can be placed over the card slot of an ATM or handheld credit card device, like those used by waiters. Using a skimmer, a thief can collect your card number and information for later use, simply by having you swipe your card as you normally would. Everything appears normal, but your personal information has just been stolen.

What Is the Cost of ATM/Handheld Skimmers Theft?

With over 400,000 ATM's located throughout the United States, ATM skimming theft costs U.S. banks as much as \$1 billion in annual losses – and the problem is rising. From 2008 to 2010, the number of cases reported to the Secret Service grew by 10% a year.¹ Combining both ATM and credit card skimming, the US Secret Service estimates the annual cost to consumers and businesses is \$8 billion.²

Information thieves can collect:

- Bank or credit card account number
- Personal name

What thieves can do with this information:

- Identity theft
- Bank fraud

ATM/Handheld Skimmers Statistics:

- Over 400,000 ATM's located in the U.S.¹
- ATM skimming costs U.S.

FTC-0001333

- PINs

banks
almost \$1 billion
annually.¹

- Cases reported to the Secret Service has grown 10% for the past 3 years.¹
- Total annual loss of ATM and credit card skimming is \$8 billion.²

¹<http://www.time.com/time/magazine/article/0,9171,2041113,00.html>

²<http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=228000267>

† Federal Trade Commission. "Consumer Sentinel Network Data Book For January – December 2011." February 2012.

† Javelin Strategy & Research. "2012 Identity Fraud Report: Social Media and Mobile Forming the New Fraud Frontier." February 2012.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub. The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)



Beware of These Scams While on Vacation

A few more weeks of summer remain, and the Federal Trade

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101



Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



NYC Restaurant Worker Accused of Identity Theft

By Drew Himmelstein
May 06, 2014

Share this



Related articles

- Hotels Warn of Credit Card Breach
- Ring Accused of Cheating Taxpayers Out of \$10M

SEE MORE ARTICLES

A Manhattan restaurant employee stole credit card information from dozens of customers and worked with accomplices to create fake credit cards and fraudulent checks in the victims' names, according to the New York County District Attorney's office.

Ilesha Jackson, 29, was allegedly part of an 11-person ring who worked together to steal the identities of customers at a midtown Hale & Hearty restaurant and make fraudulent purchases and withdrawals, according to New York County District Attorney Cyrus R. Vance Jr.

The defendants stole credit card information from at least 60 victims and made tens of thousands of dollars of fraudulent purchases and withdrawals, according to charges filed last week in New York State Supreme Court.

"Determined cybercriminals will exploit any and every opportunity to steal personal information," Vance said in a [news release](#). "These defendants are charged with using a panoply of tricks — from skimming credit cards at a popular Manhattan food chain, to forging checks, and accessing credit reports to steal even more information from their victims.

According to the indictment, Gerald Spears, 39, allegedly provided Jackson, his girlfriend, with a credit card skimmer in the summer of 2013.

Jackson used the skimmer to steal credit card information, which she provided to Spears, Vance said. Spears then shared the stolen credit card information with two other defendants, Leonce Cunningham, 36, and Samuel Santana, 36, who helped him create fake credit cards using the information. Along with other accomplices, they used the cards to make over \$90,000 in purchases, including jewelry, designer clothing and cash advances from a Yonkers casino, according to Vance.

Spears, Santana and other members of the ring also allegedly created counterfeit checks payable to an accomplice, drawing more than \$50,000 from victim's bank accounts, Vance said.

Between 2011 and 2013, Santana used stolen information to order credit reports on additional victims, Vance said. Working with accomplices, he used the information he gathered to make fraudulent withdrawals from victims' accounts and open new credit cards in their names, according to Vance. The defendants made more than \$20,000 in unauthorized withdrawals, Vance said.

The 11 defendants face multiple charges of identity theft, fraud, grand larceny and forgery.

Law enforcement officials advise consumers to order yearly credit reports, keep financial information secure and to not respond to unsolicited emails from strangers in order to avoid becoming victims of identity theft.

Drew Himmelstein is a writer and digital storyteller based in San Francisco. Her work has appeared in the San Francisco Chronicle, Dwell Magazine, American Craft and on NPR, and she is a former editor at Patch.com. She holds a master's degree in journalism from University of California, Berkeley.

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Ring

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus, Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶



rogue employee in a registrar's office created more than 300 "official" birth certificates that were fraudulent and sold them to identity thieves for as much as \$10,000 each.

Day-to-day uses of a birth certificate can also expose it to fraud. The office staff at a school, a summer camp director or the volunteer coach of a Little League team will have copies of birth certificates, often stored in haphazard ways, said Greg Sirko of VitalChek, a company that helps states distribute vital records. "We sort of created a system that lends itself in some ways to identity theft," Sirko said.

So what can be done? The speakers offered solutions that fall into three categories:

1. Restricting access

"We have pushed nationally for limiting eligibility for obtaining a birth record," said Sue Bordeaux, an Oklahoma official who leads the security committee for NAPHSIS, an association of public-records registrars. While it used to be easy for anyone to see a birth certificate, agencies across the country are now requiring that you prove you're that person or a relative before you can see the records.

While that helps, Bordeaux said, it still doesn't prevent misuse by people who have legitimate access to a birth certificate. "A lot of the fraud that we see in vital records is a family member who does it to the other person," she said.

2. States talking to each other

Sirko says fraud involving death records is becoming more difficult because states are sharing information. In the past, if you saw an obituary of a person born in another state, that obituary gave you enough personal information – like the name of the mother – to get the original birth certificate from the state of birth. Today, in many cases, the state where a person died notifies the state of birth, which can then protect the person's records.

State officials are working to build a national system for sharing death information, because the process is still too slow. "Fraudsters can move faster than government," Schwartz said. They can grab a record before we can mark it deceased."

Another agency that needs to be involved is the Department of Defense, Schwartz said. When a soldier is killed in action, the name is often broadcast widely through the media. That makes their identities a target for fraud because the military doesn't report those deaths directly to the states.

3. Verifying data, not documents

Outland specializes in document forgeries and joked that, if he was working at the department of motor vehicles or an airport security checkpoint, he would be able to catch fake documents—but people would hate him, because he would spend a long time evaluating each one and cause lines to be even longer than they are today.

As digital systems replace old paper-based ones, the focus will move away from checking the authenticity of a document and more toward checking the information that's on the document. In other words, instead of just looking at a piece of paper, officials will be able to check on whether the data written on the paper is correct and whether the person presenting the document is posing as someone else.

Government agencies are now able to check some states' databases electronically, and that ability will grow.

"The future of birth and death certificates is electronic, and we shouldn't be relying on paper," Schwartz said. "Don't try to make paper more secure. It's the information people need."

More articles you might like:



Tips to Avoid Medicare Card Fraud

Seniors just turning 65 may be surprised to find their

[Read story](#)



Authorities Shut Down Suspected Identity Theft Rin...

Whether it's a few people working together on a small-

time [Read story](#)



Consumers Feel Stressed By Data Breaches But Fail ...

Finding out that you're the victim of a data breach

[Read story](#)



Goodwill, Stubhub The Latest in Series of High-Pro...

As high-profile data breaches at Neiman Marcus,

Target, Michaels and other retailers

[Read story](#)

Displaying 4 of 10 Results. [Show More Results](#) ▶

[About](#) | [Contact](#) | [Blog](#) | [Press Room](#) | [Investors](#) | [Business Solutions](#) | [Privacy Policy](#) | [Terms & Conditions](#) | [Advertising Choices](#) | [Affiliates](#) | [Careers](#) | [Site Map](#)



Copyright © 2006-2014. LifeLock. All Rights Reserved



Services

\$1M Guarantee

How LifeLock Works

Identity Theft 101

Plans and Pricing

Identity Theft 101

Identity Theft News

Alerts

Crimes

Data Breaches

Identity Theft Protection

Basics

Children/Family/Home

Computers and Technology

Smartphones

▸ Your Money and Finances

Identity Theft Recovery

Basic Steps

Credit Score Help

Lost and Stolen Items

Understanding Identity Theft

Electronic Communication

Fraud

Social Networks

CALL US AT
1-800-607-7205

Send us an email



Secure login



ATM Overlays



Share this



:



Related articles

- Skimming Devices

SEE MORE ARTICLES

An ATM overlay is a device that is placed over the keypad of an ATM. It is often disguised to look identical to the original keypad. Overlays allow thieves to capture your PIN number as you enter it, while still allowing the original keypad to receive the PIN number as well.

How Big a Threat are ATM Overlays?

By itself, an ATM overlay is not a tremendous source of identity theft. However, when combined with a mechanism that obtains your card information – such as a skimmer, loop, camera, or other device located at the ATM – a skimmer now allows the identity thief to have access to your bank account, including both your PIN and your debit or credit card number.

What does ATM Overlay Theft Cost Consumers?

As a component of ATM theft, ATM Overlay theft contributes to the estimated \$1 billion in annual losses banks experience from ATM skimming.¹

Information thieves can collect:

- PIN Number

What thieves can do with this information:

FTC-0001342