Keep up to date with news and articles about identity theft from Consumer Federation of America and other sources.

2/5/21- Posting Your COVID Vaccine Card Online Could Lead to Identity Theft

As part of Identity Theft Protection Week, Georgia Attorney General Chris Carr issued a warning for people who have received their COVID vaccine *not* to share the news by posting their COVID vaccine card to their social media apps as doing so could lead to identity theft...

1/19/21 - IRS Opens Identity Protection PIN Program to all Tax Filers for First Time

After being in operation for nearly a decade, the IRS' Identity Protection PIN Program has been opened to all tax filers for the first time ever.
The voluntary program was first established to protect victims of identity theft by preventing fraudulent returns from being filed using their personal information. Now, anyone who has either a Social Security number or Individual Tax Identification Number and whose identify can

be verified is eligible for the program.

12/2/20 - 2021 Predictions: Government Support for Identity Crime Victims is Out and Stealing Passwords is In

The Identity Theft Resource Center's® 2021 Predictions show fundamental shifts in how identity crimes are committed, what cybercriminals want, and the resources available to help victims. Key government resources to assist identity theft victims have been eliminated and will assistance is likely to continue to decrease; cybercriminals are relying less on consumers' personal information and more on consumer behaviors to commit identity-related crimes, making personal information less valuable and attractive to cybercriminals; the ITRC believes pandemic-related identity crimes will impact victims well into 2021; and, the ITRC expects privacy, cybersecurity and identity laws to continue to merge into a more holistic set of public policies – at least at the state level.

8/26/20 - As Census Winds Down, Crooks May Ramp Up

It's really important for everyone who lives in the U.S. (and five territories) to be counted in the national census, which is only conducted once every ten years. The census information is used by the federal government to decide where funding should go for hospital, schools, roads and other services. It's also used to determine the number of seats each state has in the House of Representatives, to establish voting districts, and for many other purposes. Now that the Census Bureau says it will wind the count down on September 30 instead of October 31, as first announced, there's a scramble to collect information from people who haven't yet responded. Unfortunately, crooks may take advantage of the census to collect individuals' personal

information and use it for identity theft and other frauds. Here's what you need to know to make sure you're giving the right information to the right person and keep your identity safe.

12/11/19 - Work-from-Home Scams are on the Rise: Protect your Identity and your Wallet

When you visit sites like Indeed, ZipRecruiter, LinkedIn, or GlassDoor, you're likely to find many different companies seeking workers. Unfortunately, it can be difficult to distinguish legitimate online job offers from those placed by people who are out to scam you, especially when it comes to work-from-home jobs. Even worse, these scams have become very sophisticated. What may seem like a lucrative job that allows schedule flexibility may actually be a scheme designed to steal your money, time, and even your identity.

10/16/19 - Five Years After Settlement with FTC, LifeLock Begins to Pay Up

It's taken a while, but if you bought LifeLock's identity theft services between 2012 and 2014, you may be receiving some money from the Federal Trade Commission (FTC) soon. The FTC recently announced that it was distributing $31 million in checks averaging $29 each to more than a million consumers under a 2015 settlement with the company.

3/19/19 - Too Many Consumers Believe Theft Identity Services Can Remove Personal Data From The Dark Web

A new survey commissioned by the Consumer Federation of America (CFA) revealed that 36 percent of consumers who have seen ads for “dark web monitoring” incorrectly believe that identity theft services can remove their personal information from the dark web. An equal number (37%) mistakenly believe that these services can prevent people who buy their personal information on the dark web from using it.

1/10/19 - Free Credit Monitoring for Active Duty Military Members

Under a law that Congress passed last year, members of the military who are on active duty have the right to ask credit reporting agencies for free electronic credit monitoring services. A popular feature of many fee-based identity theft services, credit monitoring alerts people when there are changes to their credit reports such as new accounts added – information that can help them detect certain types of identity theft quickly and take remedial action.

9/21/18 - Take Advantage of Your New Right to Freeze Your Credit Files for Free

If you’re concerned about identity theft (and these days, who isn’t?), there is good news. As of September 21, 2018, you have the right to ask the consumer reporting agencies that operate on a nationwide basis to freeze your credit files and lift the freeze, whenever you want, at no charge.

5/24/18 - A Credit Reporting Agency You Probably Never Heard Of

If you have placed freezes on your credit files at Experian, Equifax and TransUnion, no one can fraudulently open a new account pretending to be you, right? Not exactly. Freezing your files at the “big three” credit reporting agencies goes a long way to protecting you from identity fraud, since most major retailers and lenders check them when consumers apply for credit. But not everyone checks consumers’ credit files at the “big three.”

4/11/18 - New Tool for Consumers to Get Help with Tax ID Theft

If someone steals your credit card and makes purchases with it, it’s not hard to solve the problem. All you need to do is contact your card issuer and the charge will be removed. If someone has your Social Security number and enough other information about you to file a false tax return and steal your refund, however, it’s a major headache. The good news is that the Internal Revenue Service (IRS) and the Federal Trade Commission (FTC) have announced a new project to make it easier for tax ID theft victims to get the help they need.

3/30/18 - Giving With One Hand, Taking Away With the Other

The Economic Growth, Regulatory Relief, and Consumer Protection Act which recently passed the Senate is mostly about eliminating important protections that were put in place after the financial crisis of 2007-2008 to avoid similar meltdowns and keep our financial system safe and sound. There’s very little for consumers in the bill, and in some cases the “consumer protections” would actually weaken people’s rights under their state laws and block the states from providing stronger protections in the future.

3/13/18 - Identity Theft, Fraud Statistics Give Consumers No Cause to Celebrate

Last week was National Consumer Protection Week, but when it comes to fraud and identity theft, consumers don’t have much to celebrate. Statistics recently released by the Federal Trade

Commission (FTC) and a private consulting company, Javelin Strategy & Research, are truly alarming. Consumers are losing lots of money – money that they could be saving and spending on legitimate products and services. They're also losing confidence in their ability to protect their personal information.

1/18/18 - Give Us Stronger Security, Not a Weak National Data Breach Law

On January 2, 2018 security company McAfee released the results of a survey revealing that consumers are worried about protecting their personal information. Of course they are! Not a week goes by without news about another data breach or an Internet-connected device that that's been spying on unsuspecting consumers. These concerns are real.

12/12/17 - Make it Harder for Fraudsters to Use Your Personal Information

It seems as though data breaches affecting millions of Americans are constantly in the news these days. If this makes you anxious about the safety of your personal information, that's understandable. You can protect your data, but when businesses have your data, you can't control how well it's safeguarded. There are some simple steps that you can take, however, to make it harder for fraudsters to *use* your personal information if they get ahold of it.

12/4/17 - Don't Let a Grinch Steal Your Online Cart

The holiday season is upon us and with it comes, decorating, baking and of course, the frenzy

of getting our gifts together. Some may choose to brave the crowds but 196 million will end up making purchases straight from the comfort of their couch. Be careful though, unless you know what to look for, you might give up a piece of your identity while grabbing that sweet deal. Let's talk about safe holiday shopping online.

11/22/17 - The Latest Uber Breach and What Should Be Done to Protect Us

The revelation that ride-hailing company Uber experienced a major data breach in October, 2016 and not only kept it secret from the customers and drivers who were affected but even paid the hackers to hush it up is another example of why we need better security for our personal information.

10/4/17 - To Freeze or Lock?

In response to the Equifax data breach, many consumers are asking the credit reporting agencies to put a security freeze on their credit files. That’s certainly a good idea if your Social Security number and other personal information were exposed in this breach.

9/20/17 - Let Consumers Freeze Their Credit Files for Free

In the wake of the data breach at the credit reporting agency Equifax, which exposed the sensitive personal information of more than 140 million Americans to identity thieves, consumer groups and members of Congress are calling for free security freezes. As we explained in a previous article on this website, the best protection from many types of identity theft that can

result from data breaches is to activate a security freeze on your credit file.

9/8/17 - What Should I Do About the Massive Data Breach at Equifax?

Yesterday, Equifax revealed that a data breach has impacted approximately 143 million American consumers. Names, addresses, Social Security numbers, birth dates, and driver's license numbers were accessed. Hundreds of thousands of consumers also had their credit card numbers exposed.

8/16/17 - Scary Data Breach Forecast

The fourth annual "Data Breach Industry Forecast" from Experian Data Breach Resolution paints a scary picture of how identity theft is evolving and the new types of security threats that we are likely to face. Companies, organizations and agencies that hold people's personal information need to be aware of these trends and harden their defenses – and so should consumers.

7/27/17 - New Ploy to Phish for People's Personal Information

In a survey that Consumer Federation of America and the North American Consumer Protection Investigators recently conducted about the complaints that state and local consumer protection agencies received last year, the San Francisco District Attorney's Office Consumer Protection Unit reported a new type of phishing scam. The perpetrators set up tables on the street, offering low-income and homeless people "free" phones, supposedly as part of a

social service program.

5/31/17 - Heartburn for Some Chipotle Customers

All you wanted was a burrito, but you may have gotten a side of data breach. Chipotle recently announced that “most of their stores” had been hit by a malware attack that aimed at gathering customers’ payment card information. So should you cry like you just ate some ghost pepper salsa or is this more like a mild pico de gallo? Let’s talk the Chipotle breach.

4/7/17 - Benefits and Limitations of Identity Theft Services

After the federal Office of Personnel Management (OPM) experienced two massive data breaches in 2015, it spent about $240 million to provide identity theft services to those affected. Was that money well-spent? To answer that question, Congress asked Government Accountability Office (GAO) to look into identity theft services and their usefulness. The GAO’s report concludes that there are both benefits and limitations of these services that should be taken into account when determining how to respond to data breaches.

2/23/17 - The Latest Way Fraudsters Are Abusing Personal Information

According to a 2016 report from the security firm ThreatMetrix, identity thieves are working a new seam in the identity theft gold mine: online lending. There is an increase in attacks against providers of alternative lending products.

1/25/17 - Massive Number of Data Breaches Reported Last Year

According to a new report from the Identity Theft Resource Center (ITRC) and CyberScout, the number of U.S data breaches tracked last year hit an all-time high of 1,013, a 40 percent increase over the 780 breaches reported in 2015. The ITRC, a nonprofit organization that provides free assistance for victims of identity theft and consumer education, has been tracking data breaches since 2005.

1/9/17 - Happy New Year, It's Tax Fraud Season Again!

This may not be what you want to hear this week, but it is entirely possible the Internal Revenue Service already has your tax return for 2016. If this is news to you, and it turns out to be true in your case, you've been scammed. As a result, your refund could be sent to an identity thief in a few weeks, and it's unlikely anything can stop that from happening.

12/19/16 - Shopping Via App? Watch Out for Fakes

This December, scammers are fooling holiday shoppers with a new high tech con. Phony retail apps are popping up in Apple and Android's app stores and stealing shoppers' personal information. Be careful when downloading new apps. Most fake apps are fairly harmless, a way to deliver spammy advertising. But some apps require shoppers to enter credit card information or provide their Facebook password. Sharing this information can open users up to fraud.

12/8/16 - Gifting a 'Smart' Device? Here's How to Keep its Recipient From Getting Hacked

In October 2016, there was a distributed denial of service (DDoS) attack that caused serious

traffic issues at major internet destinations like Amazon, PayPal and a host of other heavily trafficked sites. You may be giving a gift this holiday season that could make a similar attack possible. Spot check: Does the gift you plan to give connect to the internet? If you answered "Yes," keep reading.

10/19/16 - A Window into the Aftermath of ID Theft

Since 2003, the nonprofit Identity Theft Resource Center (ITRC) has surveyed individuals who have sought its counseling for identity theft problems to ask them how their stolen information was fraudulently used and how the crime affected them. This year's report, *Identity Theft: the Aftermath 2016™* , is even more revealing than previous ones because the ITRC dug deeper into the impact that identity theft can have on victims. It is based on responses from 300 individuals who contacted the ITRC in 2015.

9/28/16 - Lock Down Your Login to Protect Your Online Accounts

The massive Yahoo data breach is a vivid reminder that our online accounts are rich targets for hackers. They're looking for personal information that can be fraudulently used to take over our accounts, open new accounts in our names, steal our tax refunds, apply for jobs or government benefits, or send spam to our contacts. When our email or social media accounts are hacked, there is also the risk of embarrassment if something that we'd rather keep private within a circle that we define is exposed for all to see. To the extent that we use the same login information for multiple accounts (and let's face it, many of us do), the risks are multiplied.

9/23/16 - What Yahoo Users Should Do in the Face of Massive Data Breach

The news that at least half a billion Yahoo accounts have been affected by a data breach –and

that the company took two years to publicly acknowledge this – is very distressing, and not only to Yahoo users. It makes us wonder if we can ever rely on anyone who has our personal information to keep it safe. It's not just businesses that suffer from data breaches. The running list of breaches maintained by the Identity Theft Resource Center includes government agencies, schools, and healthcare providers.

9/7/16 - So You've Had a Data Breach, Now What?

Companies, organizations and agencies that hold and transmit people's personal information should keep it reasonably secure from unauthorized access and use. But what if there is a data breach that exposes the information? How should the breached entity help those affected? Should it offer them identity theft services? If so, how should it choose the provider and what features should it look for to ensure that the services will fit the needs of the victims?

8/29/16 - Five Ways Your Kids Can Get You Hacked

For adults, home is a refuge, but for children it is a never-ending treasure hunt. While you're out — you know, paying for the place — it's a safe bet your kids are getting into your stuff, and when it comes to things digital, that can be a serious problem.

8/23/16 - Privacy & Security Challenges Confronting Consumers in the Digital Economy

There are many challenges confronting consumers in the digital economy. The Internet and

digital products and services have become essential parts of our lives. Indeed, we have little practical choice about using the Internet and digital products and services. We live in a brave new world built on ever-accelerating technological advances. These advances can help make our lives easier and safer, save us time and money, spur creativity and civic discourse, and enlarge our voices individually and collectively. But they can also make us more vulnerable to commercial and government surveillance, unfair discrimination, anti-competitive practices, and identity theft and other hazards.

8/9/16 - 4 Things You Should Never Text or Email

Most of us in our “instant gratification isn’t enough” society assume that the potential fallout from transmitting sensitive information via text, fax or email is outweighed by the convenience of getting something where it needs to be fast. After all, becoming the victim of an identity-related crime isn’t the end of the world, right?

7/27/16 - Alerting Taxpayers to Possible ID Theft

In the identity theft complaints reported to the Federal Trade Commission last year, the most common use of victims’ stolen information was to commit tax or wage fraud. What’s even more alarming is the upward trajectory of this type of fraud, from 32.8 percent of identity theft cases reported in 2014 to 45.3 percent in 2015. This trend is borne out by Consumer Federation of America’s latest survey of state and local consumer protection agencies around the country, which revealed that tax ID theft was among the top three fastest-growing complaints that they received last year.

7/13/16 - Nation's Top Ten Consumer Complaints

Phony IRS agents and other imposter scams topped the list of fastest-growing complaints to state and local consumer protection agencies last year, according to the latest report from the annual survey conducted by Consumer Federation of America (CFA) and the North American Consumer Protection Investigators (NACPI). Thirty-three consumer agencies from twenty-one states participated in the survey, which asked about the most common complaints they received in 2015, the fastest-growing complaints, the worst complaints, new kinds of consumer problems, agencies' biggest achievements and challenges, and new laws that are needed to better protect consumers.

5/26/16 - Help! I Think Someone Opened a Credit Card in My Name

Maybe it's a sudden influx of subprime credit card offers in your mailbox. Or a bill from an issuer you don't recognize. Or, even, a debt collection notice regarding a charged-off account you never opened. Whatever telltale sign emerges, you now have reason to believe a credit card has been taken out in your name. While it can be hard to quell your panic, there are some steps you can take to remedy the situation and prevent further identity theft from taking place.

4/21/16 - New Survey: Half of Americans Expect Identity Theft to Cause Them a Financial Loss in the Next Year; Majority of Investment Frauds Go Unreported

Tax time is busy season for CPAs – but it's also busy season for criminals looking to steal identities and fraudulently obtain refund checks. Americans are highly aware of the threat of losing money to scammers, with half of U.S. adults (50 percent) saying that it is at least somewhat likely they will suffer some financial loss in the next year due to identity theft--and one in 10 (10 percent) say it is very or extremely likely.

4/15/16 - Why We Need a Stronger ROBOCOP on the Beat

Consumer Federation of America and Consumers Union have endorsed a new bill offered by Congresswoman Jackie Speier (CA-14), the Repeated Objectionable Bothering of Consumers on Phones (ROBOCOP) Act. The legislation aims to provide consumers with better protection from illegal robocalls and fake Caller ID. These aren't merely annoying – they are used by unscrupulous businesses and outright scammers to steal consumers' money or their personal information.

3/30/16 - Look Out for Fake Macy's Delivery Message

Each year, millions of people shop at Macy's, a huge fashion retailer with customers across North America and the world. Scammers, banking on the store's popularity, have created a new phishing con that poses as a Macy's delivery email.

3/9/16 - Are You Ready for Mobile Payments?

More and more people are using their cell phones, tablets and other mobile devices to pay for purchases. On the street in front of our office here at Consumer Federation of America, you can pay for parking with your mobile device, and you can buy coffee at the Starbucks around the corner with it, too. You can also make mobile payments at some retail stores and websites. For most consumers, the biggest benefit of mobile payments is convenience. No need to pull out your wallet for cash or plastic at the store, especially if you've got your phone near at hand anyway. No need to type in your payment information to buy something online. But what about

your privacy? Is your financial and other personal information safe? These are good questions to ask whenever you consider using new technology.

2/16/16 - FTC'S Improved Identity Theft Tools for Victims

Identity theft is a threat at any time of the year but becomes even more so during tax season. While I hope you never need them, now is the time to familiarize yourself with available resources in case you, or someone you know, becomes an identity theft victim. I've written about this issue most recently in a November 18, 2015 blog describing the IRS' new process by which identity theft victims can get a copy of a tax return filed fraudulently using the victim's Social Security number and name.
Now there are even more tools available for identity theft victims thanks to the efforts of another federal agency.

2/4/16 - Consumer Federation of America Adds Companies to its Identity Theft Service Best Practices Working Group

Consumer Federation of America (CFA) has added Equifax, ID Watchdog and Worldwide Benefit Services (ID Theft Assist) to the list of companies that are part of CFA's Identity Theft Service Best Practices Working Group. The working group, which also includes consumer advocates, helped to develop and recently revise CFA's Best Practices for Identity Theft Services.

1/20/16 - How Identity Theft Cost a Woman Her Disability Check

Many people find out their identities have been stolen when they try to file their taxes and discover someone has already used their Social Security number to get a fraudulent tax refund. In what could be considered a best-case scenario, victims of taxpayer identity theft end up dealing with an especially laborious tax-filing process and a delayed refund.

1/4/15 - IRS Proposal is Bad for Donors, Good for ID Thieves

A rule recently proposed by the Internal Revenue Service (IRS) made me scratch my head and wonder, "what are those folks at the IRS thinking?" If adopted, the rule would require nonprofit organizations to ask people who donate $250 or more for their Social Security numbers (SSNs). The idea is to make it easier for donors to substantiate such contributions. But on balance, it's a really bad idea.

12/18/15 - How to Spot the Real OPM Data Breach Letter

The U.S. government's Office of Personal Management (OPM) has been notifying those affected by a recent cyber security breach that their personal data was compromised. Unfortunately, scammers are also "notifying" consumers. Here's how to identify a real OPM notification letter and the signs of a scam.

12/14/15 - Your Holiday Identity Theft Checklist

The holiday season is a busy time of the year for identity thieves and other kinds of identity-related fraudsters. Scams abound, but if you follow a few simple rules, you can sidestep some avoidable holiday blues.

12/8/15 - H.R. 2205 is No Cure for the Data Breach Blues

Given the relentless news about data breaches, it's not surprising that members of Congress are concerned and feel that federal legislation is needed. Unfortunately, H.R. 2205, which will be considered by the House Financial Services Committee today, would not help Americans much – in fact, it would actually weaken existing protections and make it harder to enact new ones.

11/17/15 - CFA Revises Best Practices for Identity Theft Services

Today Consumer Federation of America (CFA) released Best Practices for Identity Theft Services Version 2.0 , updating the guidance that it originally issued in 2011 to encourage for-profit identity theft service providers to follow responsible practices.

11/4/15 - Better ID Theft Tools for Consumers

U.S. PIRG recently released a new report that explains how placing security freezes on one's credit reports is the only way to prevent new account identity theft. It's a proactive step that's

easy and inexpensive to take.

10/19/15 - Scam Tied to New Chip Credit Cards

Don’t have a new EMV chip-enabled credit or debit card yet? Beware emails enticing you to upgrade.

10/2/15 - When Will the Data Breaches Stop?

Another day, another disheartening news story about a data breach, this time compromising T-Mobile customers’ personal information, including Social Security numbers, addresses, and birthdates.

9/28/15 - Scam Alert -- How Scammers are Fooling Users of New App

Scammers are always taking advantage of what's new and popular. This time it's WhatsApp, a smart phone application that allows users to send text, video and audio messages via the Internet. Scammers are impersonating the app to spread malware.

9/22/15 - Got a Smartphone? Then You've Got Identity Theft Help!

Your phone is a constant, but there is something else that is also a constant which is far more troubling than forgetting your phone at home; identity theft.

9/10/15 - How to Help Syrian Refugees without Getting Scammed

Five years of conflict in Syria have displaced more than half of that country's population of 22.85 million, and, according to Amnesty International, more than 4 million Syrian refugees have fled to five countries: Turkey, Lebanon, Jordan, Iraq and Egypt.

8/28/15 - Tax Implications of Free ID Theft Services

In the past few years there has been much news about massive data breaches at mega-corporations and government agencies. Whether it is wayward hackers, state-sponsored data thieves, or the 21st century equivalent of a pickpocket, these incidents are making consumers anxious about the possibility that their personal information may end up in the hands of unscrupulous individuals.

8/20/15 - Life After Ashley Madison: How to Operate in a World Without Secrets

The other cufflink fell on the Ashley Madison hack Tuesday. According to Wired, 9.7 gigabytes of Ashley Madison data were dumped on the dark web, and the collection appears to "include account details and log-ins for some 32 million users." Where we go from here is anyone's guess.

08/10/2015 - The limits of ID-theft protection and credit monitoring

I feel compelled to write about what credit monitoring does and doesn't do to protect us after reading new information outlining how companies that are breached and then offer credit monitoring can give customers a false sense of security.

07/29/2015 - Nation's Top Ten Consumer Complaints

Identity theft topped the list of fastest-growing complaints to state and local consumer protection agencies last year, according to the latest report from the annual survey conducted by Consumer Federation of America (CFA) and the North American Consumer Protection Investigators (NACPI).

07/14/2015 - Ask Consumer Ed

Dear Consumer Ed:

My husband passed away. What steps can I take to prevent someone from accessing his information and committing identity theft?

05/14/2015 - A New Website to Help ID Theft Victims

The federal government has unveiled a new website, www.idtheft.gov, designed to provide step-by-step instructions for what people should do if they believe they are victims of identity

theft.

05/07/2015 - What a National Data Security and Breach Standard Should Do

It seems as though not a week goes by without news about another significant data breach, spurring concerns about how safe our personal information is when it's in other hands

---

04/01/2015 - Identity Theft Victim Spends 32 Days in Jail

A Georgia man says he spent 32 days in a Missouri jail for crimes a former roommate committed

---

03/19/2015 - Identity Theft Remains Top Consumer Complaint

In the Federal Trade Commission's (FTC) most recent annual complaint report, Consumer Sentinel Network for January-December 2014
, identity theft topped the list for the 15th consecutive year.

03/06/2015 - Malware Targets Android Users

Android smartphone users should be aware there is a new malware – a malicious software program – that is targeting their phones to commit fraud. Adaptive Mobile first discovered the

attack, which named it “Gazon,” and believes it has infected more than 4,000 devices.

02/13/2015 - The Biggest Threat to Your Identity This Time of Year: Loneliness

Valentine’s Day can be a pretty obnoxious holiday, particularly if you’re expecting to spend the 14th all by yourself. The constant reminders that “love is in the air,” coupled with the loneliness you might already be feeling, can make single people vulnerable to all sorts of scams.

01/26/2015 - Data Privacy Day

The National Cyber Security Alliance offers privacy tips for 2015.

01/09/2015 - It’s Tax Season. Do You Know Where Your Mail Is?

During the holiday season a missed or stolen package can be aggravating, which is doubtless why you eagerly watched for deliveries all December, calling the nanosecond you suspected a problem.

12/29/2014 - Is Sony Data Breach a Sign of Things to Come in 2015?

When the news broke that the information of more than 6,800 Sony employees including Social Security numbers, birth dates, and salaries – most consumers, including me, thought "Here we

go again" with another typical major data breach event.

12/15/2015 - Advice for Target Breach Victims

Victims of the Target data breach last year were eligible to sign up between January and April 30, 2014 for 12 months of free credit monitoring from ProtectMyID (a service of Experian). For those who enrolled early on, the free service will be ending soon.

12/02/2014 - Boost Your ID Theft Aptitude This Holiday Season

If you want to help ensure a happy holiday season — whether you own a business or are a consumer — it's time to boost your Identity Theft Aptitude because identity-theft criminals are especially active from Thanksgiving to New Year's Eve.

11/18/2014 - Identity Theft Victims Face More Than Just Financial Problems

The effects of identity theft can be traumatic and lasting, according to a report recently released by the Identity Theft Resource Center (ITRC). Identity Theft: The Aftermath 2013 is part of a series of studies, beginning in 2003, based on survey responses from confirmed identity theft victims who contacted the ITRC for assistance.

10/06/2014 - It’s Time for a Data Breach Warning Label

The breach at Home Depot is only the most recent in a torrent of high-profile data compromises. Data and identity-related crimes are at record levels.

09/19/2014 - How Your Name Could Get You Scammed

Your personally identifiable information (PII) is all around you, and much of it is impossible to protect. While your driver's license and Social Security numbers are a significant part of the equation, you can take certain protective measures to keep those from prying eyes.

08/29/2014 - Don't Get Ripped Off by Card Skimming

When you swipe your credit or debit card, there is always a risk of giving ID-theft criminals what they need to steal your money through what is known as "skimming." Criminals install electronic devices at locations at which we use cards, such as an ATM, a grocery store or a gas pump.

08/22/2014 - Another Big Security Breach

UPS has announced that it discovered a breach of its computer systems affecting 51 UPS stores in 24 states (about 1% of its 4,470 franchised center locations throughout the United States).

08/18/2014 - What's Your Identity Theft IQ?

The first step when it comes to identity theft is admitting you have a problem. Knowing your ID IQ is a good place to start.

08/01/2014 - Data Security and Consumers: Time for Action

Anyone who has watched the news over the past six months or so can attest that the issue of data security has now entered the mainstream conversation. Massive data breaches at nationally-known companies like Target, Michael's, Niemann Marcus and eBay – just to name a few – have brought the vulnerability of our nation's data security infrastructure home to millions of consumers.

07/02/2014 - Credit Monitoring Just One Component of ID-Theft Protection

Wearing a helmet on a motorcycle protects the head but leaves the rest of body unprotected. Those who sell helmets only promise protection for the head — and we expect no more.

06/25/2014 - New Coalition Forms to Serve Transitioning Vets' Financial Needs

Today Consumer Federation joined the Association of Financial Counseling and Planning Education®, Consumer Action, and Visa Inc. to announce that they have created the *Veterans Financial Coalition*
. Its goal is to help serve the needs and unique financial challenges that military veterans face when they return to civilian life.

06/11/2014 - 12 Tips to Cut Your Risk of ID Theft While on Vacation

Just as pickpockets take full advantage during vacation season, identity-theft criminals are at it, too, capitalizing on the transactions and the personal information that business travelers and vacationers create while they travel.

06/04/2014 - Adding Insult to Injury

A recent article by Sheryl Harris in the Cleveland Plain Dealer (*IRS freezes tax ID theft victims' returns – then hits them with late penalties*
, May 31, updated June 3) points to the need for the Internal Revenue Service to step up its game when it comes to helping victims of tax ID theft.

05/06/2014 - Consumers Are Paying More to Protect Their Identities

Americans are spending more on identity-theft services largely centered on alerts and monitoring, yet reported ID and data theft incidents are at near historic high levels. Target's data breach debacle has increased the debate on whether identity theft services can prevent consumers from becoming victims and if these services are worth the cost.

04/01/2014 - Tax Scam Sweeping the Nation

According to news reports, more than 20,000 taxpayers have been targeted in what the Internal Revenue Service (IRS) says is the largest phone scam that the agency has ever seen. Thousands of victims have lost money.

03/06/2014 - Get Smart: Protect Yourself, Your Friends and Your Family from ID Theft and Fraud

Identity theft is when someone steals your personal information and uses it pretending to be you, usually to get money but sometimes just to be mean. It can happen in many ways, but now that we have so much personal information on our computers, laptops, tablets and smartphones, these devices are tempting targets for ID thieves.

02/20/2014 - Alarming Rise in ID Theft

Earlier this month Javelin Strategy and Research reported the results of its latest identity fraud survey. Javelin defines identity fraud as the unauthorized use of another person's personal information for illicit financial gain.

02/11/2014 - 5 Way to Spot a Catfisher Who Wants More Than Love

Regular viewers of MTV's series "Catfish" (in which online-only, deceptive relationships are pulled into the real world, albeit with cameras running) might think that the show just highlights the extreme cases of a common problem – people who tell lies in search of a personal connection.

01/16/2014 - Dealing with the Data Breach Epidemic

It seems that every week brings bad news about another data breach. The recent revelations about breaches at Target and Neiman Marcus have heightened concerns about the collection and security of consumers' personal information.

01/13/2014 - Tax Identity Theft Awareness Week

Tax identity theft is the most common form of identity theft reported to the Federal Trade Commission (FTC) , and with the start of the 2014 tax season, the FTC named January 13-17 Tax Identity Theft Awareness Week.

01/02/2013 - The State of Identity Theft: What More Can We Do?

For thirteen years, the crime of identity theft has generated more complaints to the Federal Trade Commission than another other fraud. In 2012, more than 12 million Americans were affected by identity theft, costing the U.S. economy $20.9 billion. Every three seconds, a consumer's identity is comprised by this pernicious crime

---

12/20/2013 - Target Customers are Targeted in Massive Data Breach

On December 19 retail giant Target announced that 40 million customers' credit and debit card data may have been stolen between November 27 and December 15, during the busiest shopping season of the year. It's not clear yet how this breach happened, but it appears to have affected customers who made purchases at the company's physical stores, not on Target's website

---

12/12/2013 - Research Reveals Medical Identity Theft is Up, Affects 1.84 Million U.S. Victims

Medical identity theft is a national healthcare issue with life-threatening and hefty financial consequences. According to the *2013 Survey on Medical Identity Theft* conducted by Ponem on Instit

u
te, medical identity theft and “family fraud” are on the rise; with the number of victims affected by medical identity theft up nearly 20 percent within the last year.

11/15/2013 - Beware of Scam Emails about the Affordable Care Act

Because many people have run into problems trying to enroll for health insurance under the Affordable Care Act through the official www.HealthCare.gov website, the federal government may send emails to some urging them to try again.

10/30/2013 - Help! Credit Card Theft is Damaging My Credit Score

If you become a victim of credit card theft, it's extremely important to report the theft immediately in order to minimize any damage the charges may cause. As shown by this reader’s question, waiting to notify the card issuer may cause additional, unnecessary damage to your credit reports and scores if the fraudulent debt ends up in collections:

09/25/2013 - Avoid ID Theft and Fraud in the New Health Insurance Marketplace

Starting on October 1, 2013 people who don’t have health insurance can buy coverage through the new “marketplaces” created under the Affordable Care Act (ACA). Con artists follow the news, and even before October 1 they were contacting people asking for money, personal information, or both, supposedly to help them sign up for insurance. Here’s what you need to know to avoid these scams.

09/18/2013 - New Oregon Law Aims to Protect Child ID Theft Victims

Child identity theft is a serious problem – a study issued earlier this year estimated that one in 40 households with minor children has experienced the theft and misuse of at least one child's identity. Children are tempting targets for identity thieves because their personal information is unblemished; they have no criminal records and no bad credit.

09/09/2013 - How a Stolen Phone Can Affect Your Credit

You've enjoyed a great day out – shopping, grabbing a coffee with friends, maybe a quick stop at the park to walk the dog. But then as you walk into the house, you have a sudden panicked feeling … where is your cellphone?

08/26/2013 - Put Protecting Your Child's ID on Your Back-to- School To-Do List

Schools collect a lot of personal information about students – information that, in the wrong hands, could be used for identity theft. Children and young adults are tempting targets for identity thieves because they usually have unblemished credit histories and no criminal records. Fraudsters can use their Social Security numbers and other personal information to open credit accounts, apply for jobs, rent apartments, obtain medical services and, even scarier, to impersonate them if they get into trouble with the law.

08/19/2013 - Don't Let "Breach Fatigue" Risk Your Identity When Data Breach Events Occur!

Based on my over 20 years of ID theft and data breach experience, I have concluded that brea ch fatigue

has relegated most data breach news events from front page headlines to the back pages, reflecting a lesser news value and a place of insignificance.

08/05/2013 - Mobile Health and Fitness Apps: What Consumers Need to Know

Consumers have access to ever increasing numbers of mobile apps providing health, fitness and wellness information. Many consumers might assume that entering personal information, and especially personal health information, to gain access to the information would be very protected. That assumption needs to be reconsidered in light of excellent reports recently issued by the Privacy Rights Clearinghouse (PRC).

07/24/2013- 9 Things You Need to Do When Your Email is Hacked

For many people, the first sign that their email has been hacked comes when a friend shoots them a text or an email saying, “Hey there. Uh… I think your email was hacked… unless you meant to send me that link to the Viagra store.” Or you might figure it out because you can no longer log in to your account, or your smartphone can’t retrieve your messages. Or maybe you can log in to your email, but find that your inbox is suddenly empty and all of your contacts have been deleted. No matter what tips you off, when your email is hacked (notice I say when, not if, here), the impact can be disastrous.

06/05/2013- Progress on Identity Theft Services Measuring Up to CFA Best Practices

ID Theft Services Make Changes to Provide Clearer Information on their Websites and Avoid

Overpromising How They Help Consumers

Since Consumer Federation of America (CFA) issued its April 2012 report, Best Practices for Identity Theft Services: How are Services Measuring Up?, which analyzed how well identity theft services provided key information to prospective customers on their websites, many of the services that were studied have made significant improvements. CFA's analysis and recommendations were based on the voluntary guidelines, Best Practices for Identity Theft Services, which the organization developed in 2010-2011 with the help of theft service providers and consumer advocates.

05/15/2013- Slam the Door on Phishing Scams

Consumer Federation of America (CFA) has released new tips, *Slam the Door on Phishing Scams*, and a short, funny video to help you spot and avoid phishing. It's when crooks, pretending to be from well-known companies, organizations, or government agencies, contact you and try to trick you into revealing your Social Security numbers, financial account information, passwords, or other personal information. That information is then used to make unauthorized purchases, take over your accounts, open new accounts in your name, get tax refunds and other government benefits, and even apply for jobs.

05/08/2013- Understanding the ID Theft Industry and Choosing the Right ID Theft Service Provider

It seems like a day does not go by without being inundated by radio and TV advertisements or unsolicited mail and email to sign up for some type of an ID Theft protection program. This article will serve as a crash course in understanding the ID Theft industry and how to choose the right ID Theft service provider for you and your family.

4/16/2013- Free Resources to Support Identity Theft Victims

Identity theft is a serious problem – the Federal Trade Commission estimates that there are 9 million victims each year so it's important for organizations to know there are free resources that they can use to help individuals they serve who have problems resulting from identity theft, even if they have limited professional experience dealing with this issue.

4/04/2013- Don't Be Mislead by Fake IRS Websites

As the deadline looms for filing your taxes, there is a heightened identity theft risk, with many tax schemes designed to steal identity information, tax refunds, and more.

3/27/2013- Watch Out for Affordable Care Act Scams

If you get a call or an email from someone who claims to be from the government and asks for your personal information in order to send you a new "national medical card" or sign you up for coverage under the Affordable Care Act, beware!

3/20/2013- Social Security Considers New Policy to Help Child ID Theft Victims

On February 11, the Social Security Administration (SSA) published a Request for Comments on proposed changes to its policy for assigning new Social Security Numbers (SSNs) to children age 13 and under in the Federal Register (78 FR 9765). Comments are due on April 12th.

3/12/2013- An Apple a Day May Not Keep the ID Thieves Away

We read with interest a report earlier this year from Identity Theft 911, an identity theft service provider, concerning complaints that it received from subscribers about unauthorized purchases made through the online Apple store. The fraudsters apparently took advantage of an offer to provide consumers with “instant credit” through Barclaycard.

3/04/2013- Taxpayer Tips for Protecting Your Identity: IRS Resources

Every tax season brings news stories about thieves filing fraudulent tax returns and getting refunds using stolen personal and financial information.

Other than being concerned, is there anything taxpayers can do? The answer is "yes". And they can do so with help from the IRS which has instituted a number of processes for combating identity theft and assisting taxpayers who are, or may become, identity theft victims.

2/26/2013- Do You Know a Scam Website When You See One?

Jamie May, VP of Customer Support and Chief Investigator, AllClear ID

There are literally thousands of scams and misleading websites out there, with new ones created every day. As a consumer, a key to protecting your identity is to learning to identify these scam websites so you can protect yourself when online.

2/19/2013- What You Need to Know About Tax-Related Identity Theft

Raul Vargas, a Fraud Operations Manager at IDentity Theft 911's Fraud Resolution Center

Tax day is months away, but take steps now so you can file your return early—before identity thieves beat you to the punch.

Many victims of tax-related identity theft uncover the fraud after they have filed their returns, leading to delayed refunds and additional problems with the IRS and Social Security Administration. One way to stay ahead of the bad guys is to file your taxes early.

2/4/13- 9 Ways Disconnecting Doesn't Make You Any Safer

A funny thing happened on my way from Los Angeles to Washington, D.C. – I found myself on a flight without Wi-Fi. The prospect of being unplugged for more than four hours on a flying machine without the ability to communicate with (or distract) colleagues, with zero information from the outside world – let's just say I almost lost it.

I had two newspapers and a book by my favorite fiction writer, Vince Flynn, but I was not connected. And somehow, the thought of being alone (even though I was on a full flight) for a large chunk of time was daunting. And, let's face it, the fact that we've all become so co-dependent – with MACHINES – is kind of pathetic. But here we are.

1/25/13- Medical ID Theft - It's Not Just About the Financial Risk

By Robert Greg, CEO, ID Experts, and Robin Slade, Development Coordinator for the Medical Identity Fraud Alliance and CEO & President of the Foundation for Payments Fraud Abatement & Activism (FPF2) and FraudAvengers.org

Medical identity theft is among the most devastating and dangerous of identity-related crimes perpetrated against consumers. It occurs when someone misrepresents who they are in order to obtain health-related services. Or alternatively, a healthcare provider, either real or someone just using a valid provider number, bills for medical goods and services never rendered using someone's fraudulently obtained medical ID. When someone steals your medical identity your protected health information (PHI) can become contaminated with the thief's medical information. This can lead to misdiagnosis and potentially put your life at risk.

What if you're given the wrong blood because your records indicate another person's blood-type? What if you receive a drug you are severely allergic to because the records are incorrect? What if your appendicitis goes undiagnosed because your medical records state your appendix has already been removed?

1/18/13- Seniors Beware! Latest Medicare Scam

By: Debra N. Diener, *J.D.,* CIPP/G; blog at *Privacy Made Simple*

Scammers are shameless and prey on anyone and everyone.

So this alert is for seniors so you can protect your private personal and financial information. If you're not a senior, please share this alert with any seniors you know so they can protect themselves.

1/11/13- Survey Sheds New Light on the Scope and Consequences of Child Identity Theft

By: Joanna Crane, Federal Trade Commission.

Child identity theft has seen an increase in public awareness, legislative activity, and research in the past few years. The Federal Trade Commission and Department of Justice's Office for Victims of Crime's 2011 forum, Stolen Futures: A Forum on Child Identity Theft, identified several unique challenges around the prevention and detection of, and recovery from, child identity theft. Yet no reliable metrics were available to help understand the scope of the problem. Three studies were discussed, but they were non-scientific reports, so the data they provided could not be projected to the general population or used to estimate the total number of child identity theft incidents.

ITAC, the Identity Theft Assistance Center, a nonprofit supported by financial services companies, and Intersections, Inc., a provider of identity management services, commissioned Javelin Strategy & Research to conduct a survey to get more accurate statistics about the crime. The goal is to share the information with others in government, child advocacy, and financial services to help stakeholders develop solutions to protect children.

12/31/12 - Is Your Small Business At Risk of Small Business ID Theft?

By Mark Pribish, Vice President and ID Theft Practice Leader, Merchants Information Solutions, Inc.

Most people believe ID Theft is only a problem for individual consumers.

However, the current environment of cybercrime, data breaches and the insider threat have put a target on the backs of small businesses – where small business identity theft and fraud has become a new and emerging risk management issue.

So let's begin with what we know:

- Small Businesses handle sensitive customer and employee information including social security numbers, driver's license numbers, birth dates, and bank/credit union account information.
- Small Businesses use e-mail, computerized accounting, electronic procurement, and stores electronic employee and customer information.

Now here is some information you may not know:

12/10/12 - Watch Out For Holiday Scams

By: Jamie May, VP of Customer Support and Chief Investigator, AllClear ID

The holiday season is quickly approaching, and it can bring with it a variety of online, email, and social media scams. This year, retailers aren't the only ones who want us to spend our money, so do scammers. To ensure you don't fall victim to any scam or gift-purchasing hoax, watch out for these 2012 holiday scams:

Craigslist/eBay Purchases – Typically, if you're careful, it's safe to purchase on these sites. However, during the holiday season, since the hottest toys and gadgets for will sell out fast, scammers will "claim" to be selling these items at an extremely high price on sites like eBay and Craigslist, only to take your money and run. To avoid this, try to shop locally on Craigslist and to meet the buyer in person. Don't ever wire a payment (wired payments are tough to trace and even tougher to get a refund on). On eBay, research vendors extensively. If your gut tells you that something isn't right, then listen and find a better way to make your purchase.

11/21/12 - Top Tips From Itac For Safe Online Shopping

Online shopping is easy and convenient, but fraudsters take advantage of shoppers who are eager for a bargain or exploit security vulnerabilities in your computer's software. The best way to stay safe is to put security measures in place before connecting and by understanding the consequences of online actions. The Identity Theft Assistance Center (ITAC) offers these tips on how consumers can stay safe while shopping online this holiday season...

10/31/12- Don't Be Deceived By Imposters on the Phone

By: Carri Grube Lybarker, Administrator, and Juliana Harris, Communications Coordinator, South Carolina Department of Consumer Affairs

Every year, thousands of consumers fall victim to telephone scams. While there are legitimate companies who use the phone to offer their products and services, con artists use it as a tool to commit fraud. Telephone scams can take many forms, but they share the common element of trying to separate you from your money or compromise your personal information.

We have received an increasing number of reports from South Carolina consumers about imposter telephone scams. Fraudsters pose as different businesses or government agencies to try to trick people. For example, a caller may pretend to be a debt collector and ask you to provide your financial account information over the phone to settle a debt for less than the full amount. You may not be sure you owe the debt – and in many cases you don't. But the offer is time-sensitive; you must act now for the debt to be forgiven! Sometimes these scammers pretend to be from state or federal agencies, including law enforcement agencies, to gain your trust or intimidate you.

10/19/12 - Your Identity is On(the)line: The Risks of Smartphones and Identity Theft and How You Can Protect Yourself

By: Sean Naron, Administrative and Advocacy Associate, Consumer Federation of America

According to a Javelin Strategy & Research survey, identity fraud (the actual misuse of illegally obtained personal information) in the U.S. increased by 13 percent in 2011, with more than 11.6 million adults becoming victims. What's even more frightening is that the personal information that you store on your smartphone is now a tempting target for ID thieves.

In fact, the survey found that smartphone owners were a third more likely than the general population to be victims of identity fraud. This may be due, at least in part, to consumer behavior: according to Javelin, 32 percent of smartphone owners don't update to a new operating system when it becomes available, 62 percent don't use a password on their home screens, and 32 percent save their login information right on their devices.

How should you protect yourself and your phone from identity thieves?

10/12/12 - Be on the Ball When You Get a Telemarketing Calll

By: Administrator

Recent enforcement action by federal bank regulators against Discover Card is a remi

---

10/01/12 - F ifth Annual Protect Your Identity Week Campaign Targets ID Theft Protection When Using Mobile Devices

By: Gail Cunningham, Vice President of Membership and Public Relations, National Foundation for Credit Counseling

Being in first place usually brings with it bragging rights, but not if it's the top spot in the Federal Trade Commission's annual complaint report. For the 12th year in a row, identity theft has held that dubious distinction, as ID theft complaints once again topped the 2011 list. Of more than 1.8 million complaints filed in 2011, 15 percent were related to identity theft.

09/18/12 - Rollback that Text: A New Texting Scam Advertises Free Walmart Giftcards

By: John Sours, Administrator, Cathy Mendelsohn, Media Specialist, and Lauren Simons, Legal Intern, Georgia Governor's Office of Consumer Protection

Recently our agency received a question from a Georgia consumer about whether the text message she had received claiming she'd won a Walmart gift card was legitimate or not. The fact is, it is highly unlikely that this kind of text message is legitimate.

Scams involving purported “free” gift cards have been reported throughout the country. In March, the Better Business Bureau reported a scam in which many people received text messages promising “free” Walmart and Best Buy gift cards. One such message read, “Walmart $1,000 gift card for the first 1000 users to go to [link] and enter code 2938.” Another said, “You have been randomly selected for a Best Buy gift. Get your $1,000 gift card at [link].” Neither of these offers panned out.

08/28/12- Getting Ready for Back to School? Learn How to Protect Your Child’s Personal Information

By: By: Steve Toporoff, Attorney, Division of Privacy and Identity Protection, Federal Trade Commission

As back-to-school time approaches, children may be thinking about meeting up with friends to share stories about their summer adventures. But when it comes to personal information, parents and kids need to be careful about sharing too much. These days the casual use of sensitive data (like a Social Security number on a registration form, permission slip, or health document) can lead to child identity theft, a serious crime that impacts thousands of kids each year. Parents can take steps to protect their children from ID theft with free resources from the Federal Trade Commission (FTC).

08/20/12 - Identity Thieves Reaching Into the Great Beyond

By John Breyault, National Consumers League

Identity theft is a major problem for consumers in the United States. In 2011, the Federal Trade Commission (FTC) received 279,156 complaints about identity theft, more than any other complaint category. And that represents only those who knew enough to complain to the FTC. According to a survey by Javelin Strategy & Research, 11.6 million adults became victims of identity fraud – that’s the use of one’s stolen information – in 2011, an increase of 13 percent

from the previous year.

Over the past few years, identity thieves discovered a new and practically riskless form of identity theft – filing fraudulent tax returns with stolen personal information. In 2011 alone, the Internal Revenue Service (IRS) stopped 262,000 tax returns and $1.4 billion in refunds because of identity theft. It is unknown how many others slipped through, but surely the problem is massive. Recently an audit by the Treasury Inspector General for Tax Administration estimated that identity theft may cost the IRS $21 billion over the next five years.

08/09/12 - Gone Fishing?

By: Administrator

Here at Consumer Federation of America we use a spam filter that catches dozens of phishing emails every day. But some still get through. Phishing is when an identity thief pretends to be from a company, organization, or government agency, and asks you to provide your personal information for some reasonable-sounding purpose, or tries to get you to click on a link that allows a thief to get into your computer remotely and steal account numbers and other information. Recently a staff person at CFA received an email that appeared to be the monthly bill from her wireless phone company. The amount of the bill was higher than usual, though, which caused her to look more closely at the message. She noticed that the sender's address was " alerts@irs.gov ," which made no sense. A call to the wireless company confirmed that this was not her bill. If she'd clicked on the link to pay it, it probably would have taken her to a fraudulent website made to look just like the company's, where she would have provided her credit card number. Spyware might also have been installed in her computer.

07/03/12- Fighting and Fixing Identity Theft: FTC's Helpful Consumer Tools

By: Guest Author Debra N. Diener, J.D., CIPP/G. Privacy and Identity Management Expert, Blogger at privacymadesimple.net

Identity theft continues to be a pervasive crime with devastating impacts. It's a crime that's committed from many different angles which is why I've written about specific aspects of it in prior blogs. There are always new scams emerging.

Becoming a victim of identity theft is terrible enough but then you have to figure out what to do --- and that can become a complex process. The criminals often use the stolen identity information themselves for multiple crimes and then may sell it to others. The multiple crimes make it even harder since you may have to deal with more than one office or agency to untangle and repair the damage that's been done

---

6/22/12- On Twitter? So Are Scammers.

By: Guest Author, John Breyault, National Consumers League

Many consumers find the popular social media site, Twitter, useful for staying in touch with friends and family and getting updates from organizations or famous people. Unfortunately, scammers see the millions of Twitter users very differently: as potential targets.

Scams on Twitter usually involve some kind of link or promise from either a user you don't know or a user whose account has been compromised.

5/21/12- How Does Identity Theft Impact Older People?

By: Administrator

That's the question the Federal Trade Commission (FTC) is asking as it plans its law enforcement agenda, policy work, and public education efforts for the coming months. Seniors may be particularly vulnerable to identity theft. For one thing, they tend to be trusting, which could make them more susceptible to "phishing" scams in which identity thieves, pretending to represent familiar companies, organizations or government agencies, ask to confirm their personal information.

4/18/12- How Are Identity Theft Services Measuring Up to Best Practices?

By: Administrator

Today Consumer Federation of America (CFA) released Best Practices for Identity Theft Services: How Are Services Measuring Up?
, which analyzes how well identity theft services are providing key information to prospective customers. The study is based on CFA's
Best Practices for Identity Theft Services
, voluntary guidelines that CFA developed with the help of identity theft service providers and consumer advocates. Released last year, the best practices resulted from CFA's first
study
of identity theft services in 2009, which raised concerns about misleading claims about the ability to protect consumers from identity theft, lack of clear information, and other troublesome practices.

4/6/12- Do You Know the Identity Theft Risks on Social Networking Sites?

Guest Post by: Nikki Junker, Social Media Coordinator, Identity Theft Resource Center

Social networking has become a mainstay in the everyday lives of many consumers, with over 800 million people reportedly using Facebook on a monthly basis. The risks of privacy intrusions and identity theft, however, may not always be apparent to social networkers. At the

Identity Theft Resource Center, we have become concerned about a correlation between identity theft and Facebook use. Recently the ITRC conducted a survey to measure Facebook users' understanding of the possible risks and threats.

3/20/12- Data Breaches: Panelists Offer Tips to Companies on'Mending Fences' Following a Data Breach

Guest Post by:Bloomberrg BNA Privacy and Security Law Report

Good communication with customers, regulators,and others is critical following a data breach, panelists emphasized March 8 at the International Association of Privacy Professionals Global Privacy Summit. Sixty-three percent of the cost of a breach is attributableto lost business, according to a 2010 study by the Ponemon Institute (10 PVLR 418, 3/14/11).

That percentage includes both lost customers and the failure to acquire new customers, Joanne B. McNabb, chief of theCalifornia Office of Privacy Protection, explained. Lisa J. Sotto, partner and head of the Privacy & Information Management Practice at Hunton & Williams LLP, in New York City, added that the Securities and Exchange Commission disclosure guidance urging companies to include data security risks and security incidents in their reports to the SEC (10 PVLR 1495, 10/17/11) could hurt a company's stock value.

2/22/12- Don't Let Thieves Steal a Piece of Your PII

By: Matt Cullina, Identity Theft 911

Of all the things you pray you never lose, I'll bet your library card isn't one of them. What's the worst that could happen?

Last summer, a California woman found out – to the tune of $643. Someone used her card to check out books, and never brought them back. Since the woman didn't cancel the missing library card, she got slapped with the lost-book fines.

Those missing books can teach us a powerful lesson: Our personally identifying information—or PII—is everywhere, and identity risks exist in situations (like a lost library card) that we'd never think twice about.

1/30/12- Zapping Identity Breach Problems

By: Administrator

The recent announcement by online shoe-seller Zappos that a hacker may have gained access to some of its customers' data is a reminder that our personal information can be vulnerable even if we shred our documents, put our bill payments in public mailboxes, use firewalls and anti-virus and anti-spyware on our home computers, and take the other recommended steps to protect it. When we provide our data to others, it's up to them to keep it safe.

1/19/12- Don't Let Skimmers Steal Your Cash

By: Bo Holland, Founder & CEO, Debix | AllClear ID

Identity thieves are placing credit card skimming devices everywhere, but particularly on gas pumps and on outdoor ATMs. These devices are small and hard for the typical person to detect, but they can be financially lethal. Skimmers are designed to capture credit and debit card information when one is scanned through for a purchase, and then they either transmit the information via a Bluetooth device to a nearby laptop, or store it locally for the thief to pick up at a later date. This information can then be used online or uploaded onto a counterfeit card for making purchases.

12/27/11- Make a New Year's Resolution to Check Your Credit Reports

By: Administrator

The start of the year is a good time to get organized and take care of all those little things that you've been meaning to get done. One easy thing you can do is request your credit reports. Just like a physical check-up, it's a good idea to check your credit reports regularly to correct any errors that could affect your credit health and spot signs of possible identity theft.

11/21/11- Have a Jolly, ID Theft-Free Holiday Season

By Guest Author Mark Pribish, Vice President and ID Theft Practice Leader, Merchants Information Solutions, Inc.

The holiday season is prime time for identity theft criminals. Your name, address, and phone number, your date of birth, your Social Security number, driver's license number, health insurance number, student ID number or employee ID number, your financial account numbers, your passwords – these bits of information can be like presents under the tree for identity thieves who know how to use them for their own fraudulent purposes.

By following these ten easy tips during the holiday season and throughout the year, you can reduce the possibility that you or your family members could become identity theft victims.

11/10/11- An Apple a Day Keeps Identity Theft Away

By: Administrator

When you go to a doctor for the first time, you'll be asked to fill out forms with all kinds of personal information. Sometimes that will include your Social Security number. Patients often want to know: do I really have to give this information to the doctor's office? This is not an easy question to answer.

10/14/11- Stolen Innocence: Child Identity Theft

By: Guest Author Matt Cullina, Chief Executive Officer, Identity Theft 911
Identity theft doesn't just strike adults – kids and teens are prime targets for identity thieves. The Federal Trade Commission reported that victims age 19 and under accounted for 8 percent of the identity theft complaints that it received in 2010. And a Carnegie Mellon University report issued earlier this year provided disturbing evidence that children are deliberately being targeted for identity theft. Why are children vulnerable and how can they be protected?

9/29/11 - X Marks the Spot: Mapping Medical ID Theft

By: Administrator

They say a picture is worth a thousand words, and the interactive map of medical identity theft occurrences in the United States recently created by the World Privacy Forum paints a vivid picture of the hot spots for this crime.

9/20/2011 - WellPoint/Anthem Blue Cross Applicants Eligible for Class Action Lawsuit Settlement

By: Administrator

Consumers who applied for health insurance coverage through WellPoint/Anthem Blue Cross before March 10, 2010 may be eligible for court-ordered benefits under the settlement of a class action lawsuit.

9/14/2011 - Scams Could Leave Disaster Victims Hanging Out To Dry

By: Administrator

Hurricane Irene was a jarring reminder that communities in the United States can be vulnerable to devastating damage from wind and rain. Irene destroyed roads and homes and left hundreds of thousands without power for days. Texas has been plagued by wildfires that have blazed across thousands of acres and demolished more homes than any other single fire in Texas history. Even while the victims of these natural disasters are in dire need of assistance, they could be at risk for another, man-made disaster: identity theft.

9/7/2011 - Consumer Federation of America Unveils New ID Theft Website IDTheftInfo.org Features Best Practices for ID Theft Services, Other Resources.

Washington, D.C. – Today, Consumer Federation of America unveiled a new website, www.IDTheftInfo.org, which features CFA's Best Practices for Identity Theft Services and other resources for consumers and businesses. "IDTheftInfo.org is an easy-to-use gateway for information about identity theft from Consumer Federation of America and other reputable sources," said Susan Grant, CFA's Director of Consumer Protection. Visitors to the site can take quizzes to test their ID theft savvy, learn how to protect themselves, and find information about what to do if they become ID theft victims. Advice for businesses about data security is also provided. The "Latest News" section of the website will keep people informed about identity theft-related issues and developments.

3/11/2011 - CFA Issues Best Practices for Identity Theft Services to curb misleading claims about how identity theft services can protect consumers and encourage clear, accurate information about the help they provide.

With security breaches and identity theft cases frequently in the news, consumers are worried about becoming identity theft victims. Responding to this concern, dozens of companies offer identity theft services. In 2009, Consumer Federation of America (CFA) took a critical look at for-profit identity theft services and identified some serious problems, including misleading claims about preventing identity theft, unclear information about how services worked, and exaggerations about what guarantees or insurance provided. Today, CFA released Best Practices for Identity Theft Services, which were developed with a working group consisting of identity theft service providers and consumer advocates…