

[Click to view this email in a browser](#)

Identity Theft Resource Center



itr@c News - Q2 2009

A Message from the ITRC

The ITRC is excited to announce our new toll-free, no-cost victim assistance number: 888-400-5530. It has been a long sought after goal of the ITRC to be able to provide victims with toll-free access to the ITRC call center.

In addition, the ITRC has made some notable changes and updates to its website. This includes a *Help I'm a Victim* button and page, a new data breach section updated weekly, a new scam alert section and a RSS feed from TrendMicro. To check out these new changes, go to www.idtheftcenter.org

Is Anyone Safe from Identity Theft

Part II – Pro-Active Measures for the Consumer

As we said in the inaugural issue of the itr@c news, the answer to this question is no. Faced with the reality that your personal identifying information (PII) is "out there", you can now clearly understand why we say you do not control the access to your personal information. The protection of your identity requires you to take pro-active steps to minimize your risk.

Consumers are faced with a wide range of products and services that offer or suggest that they can protect you from identity theft. It falls to the consumer to evaluate the claims and services and make their best judgment as to which ones serve their needs. With that said, there are



In This Issue

- [What are the types of Identity Theft?](#)
- [Is Anyone Safe from identity theft?](#)
- [The Sandbox](#)
- [ITRC 2008 Victim Survey](#)
- [For the Consumer](#)
- [Scam Alerts](#)
- [The Romance of Identity Theft](#)
- [Legislative Updates](#)

What are the Types of Identity Theft?



services currently available to the consumer at no-charge. These include the government-mandated programs such as Annual Free Credit Reports, "fraud alerts" and consumer statements. For a minimal fee, consumers may also place credit/security freezes. In addition, there are many consumer products available for purchase. However, in this issue, we will address only those products readily available to consumers and victims at no-charge or only minimal fees.

In 2004 Congress approved a law that allows each individual a free credit report from each credit reporting agency (CRA) every 12 months. The three nationwide CRAs have set up one central

website, toll-free telephone number, and mailing address through which you can order your annual report. To order a copy of your report, go to www.annualcreditreport.com or call 877-322-8228. This does NOT take the place of the laws that allow individuals to receive free reports if they are denied credit, discover there are errors in their reports or suspect identity theft. You do NOT need to purchase any additional services unless you wish. If you have any questions about the new federal free credit report program, please contact the ITRC at itrc@idtheftcenter.org (toll-free at 888-400-5530) or the FTC at 877-FTC-HELP (www.consumer.gov/idtheft).

The Fair Credit Reporting Act (FCRA) allows everyone to submit a "consumer statement", up to one-hundred words, explaining their version of a dispute or situation. A "fraud alert" is a consumer statement added to your credit report asking issuers to check with you prior to issuing credit. Unfortunately, at this time, while there is a law that requires issuers to honor this request, some credit issuers do not obey the law. Other credit issuers don't use credit reports so they do not see the fraud alert. Again, consumers can place a fraud alert for free. It lasts for 90 days, and is renewable. However, if you are a victim of identity theft and have submitted a police report to the CRAs, it can be extended to seven years.

Credit/Security freezes are a stronger measure consumers may make to minimize a thief's access to personal information. All states now have credit freeze programs, but not all programs are the same. They vary from state to state, depending on the laws that state has passed, or if the freeze is being offered by the three Credit Reporting Agencies. Please see our State and Local Resource Map for your states freeze law. Potential creditors, insurance companies, landlords and some employers doing financial background checks may be told that your report is unavailable for viewing.

Placing a fraud alert or credit freeze will not affect your credit score but both will prevent you from getting "instant" credit. That is the trade-off for higher levels of information security. In ITRC's opinion a freeze is the best form of financial identity theft protection currently available, but it is by no means a guarantee of safety. For example, companies can, and will, issue credit without looking at a credit report. However, you have a very strong argument as to the fraudulent nature of that account. Also, a credit freeze will not stop or fix an ongoing identity theft. For many of us, a freeze not only brings peace of mind but provides some measure of control to our financial security.

It should be noted, that identity theft ranges from financial new account openings to someone creating a criminal record in your name. There may be medical debts created, fraudulent checks written, government benefit fraud, or account takeover. These are examples of some of the issues you need to be aware of when evaluating any product or program currently available.

Annual Credit Reports are an effective means of monitoring your credit reports, especially when staggered throughout the year. However, they do not prevent financial identity theft nor will it notify you of criminal identity theft, governmental fraud or check fraud.

Financial Identity theft occurs when an imposter gains access to personal identifying information (PII) and uses it for personal gain: This could include: new lines of credit, loans, and mortgages; new accounts, account takeover, or checking/debit fraud; and Tenancy and/or utilities. This is the most common view of "identity theft" most prevalent in today's marketing, advertising, and media coverage.

Governmental identity theft could be defined as when a thief uses another persons PII to obtain employment, governmental services, benefits, or IRS refunds, to name just a few. This type of identity theft has a significant and far reaching impact on its victims. For instance, the victim finds out when their tax return is held by the state or a court orders wages withheld from the victim.

Criminal identity theft occurs when the thief provides someone else's PII to avoid: personal background checks; law enforcement scrutiny and/or criminal arrest; or child support.

Perpetrators often use a false identity because they could not pass a required background check and they may use false identities to escalation of charges due to previous probation or parole.

A new term being used is "assumption". Assumption is defined as when the imposter, or criminal, is using the victim's identity for multiple purposes such as employment, medical and financial identity theft. Essentially, this person has "assumed" the victim's entire public identity.

The Sandbox

A fraud alert will not prevent someone from passing bad checks. It has no impact on a criminal record or government benefit application. It may not affect someone getting a job as you. It will however clearly warn creditors to check with you before opening new accounts.

A credit freeze will not prevent the above-mentioned types of identity theft issues but it will prevent a creditor from seeing your credit report for the purposes of opening a new account. As we said in Part I of this series, you have shared parts and pieces of your identity for years with schools, medical facilities, employers, and financial institutions, just to name a few. The risk of your PII being potentially exposed by data breaches rises almost daily. The point is identity theft is not just a financial crime. Identity theft is an ever-expanding crime and brazen criminals find a multitude of ways to use information fraudulently.

Identity theft is a crime that can cause a great deal of harm if not dealt with in a timely manner and if the victim doesn't know the proper steps to take. With the right assistance and information, the problems it causes may be mitigated. Experts agree that identity theft cannot be prevented, but the risk of it happening to you can be minimized. There are thousands of ways to steal an identity, and some of these are beyond your control, and certainly beyond the control of a single product.

In the next issue of itr@c news, we will address other consumer products which are currently available to consumers for purchase.

ITRC Travel Tips

For Business and Vacation Travel

Whether you travel for business or pleasure, a traveler must be on the alert for opportunities that an identity thief may try to take advantage of in any given situation. Unfortunately you cannot trust anyone you meet (housekeeping staff, bellmen, security guards, front desk clerks, etc) with your personal information.

The following items should be taken into consideration before and during travel:

- Checks - Leave checkbooks and checks at home, in a locked safe. ITRC recommends that you use cash, traveler's checks or credit cards for purchases.
- ATM/Debit cards/Credit Cards – Consider restricting the use of your ATM card to securely located Automated Teller Machines.

Fake ATM machines are known to have been placed in high traffic tourist areas. Debit cards also provide thieves with a direct pipeline to your bank accounts. When used with a PIN, you need not sign for the purchase. When used for a "credit" purchase with a signature, no confirming PIN is needed. This is why debit cards are deemed valuable to thieves. It is more difficult and time consuming to resolve fraudulent purchases made with debit cards.

ITRC recommends using credit cards while traveling. Only credit cards are protected by federal law as to the amount of money that you are responsible for if lost or stolen, and most companies now extend a zero liability policy to customers.



Down Economy - Surprising Impact on Crime

by Julie Ferguson
Vice President of Emerging
Technologies, Debix

Surprisingly research shows that violent crimes, such as murder, decrease in a down economy. Conversely, fraud, such as identity theft, actually increase. Experts state the reason for this may be when the economy goes bad, many people move in with parents or relatives, and they stay home more — both of which appear to have a calming effect. The increase in fraud happens as people begin to rationalize that fraud is easy to commit and doesn't really hurt anyone.

Expert W. Steve Albrecht associate dean at the Marriott School of Management at Brigham Young University, further explains "People commit fraud because of three factors: financial pressure, the perception of an opportunity, and rationalizing it as O.K. This is the fraud triangle... All three of these elements have been increasing. Being at the down part of an economic cycle exacerbates the problem."

According to San Diego Police Chief, Bill Lansdowne "Domestic violence, alcohol-related crime, white-collar crime is starting to increase," he says. "Identity theft, mortgage fraud, senior abuse, too — people taking advantage of seniors, trying to get to their money." San Diego's murder rate is the lowest it's been in a decade — and it's holding steady. But Lansdowne says these other crimes are starting to trouble him.

About Julie Ferguson:
Board Member, ITRC
Council Member, ANSI-IDSP
Co-Founder, Merchant Risk Council

For additional information, click [here](#) for the ITRC Fact Sheet 131 Credit Card vs. Debit Card

- Leave bills at home - Business travelers often take advantage of quiet evenings in hotels to catch up with bookkeeping and paying bills. Unfortunately many people have access to your room while you are at meetings and victims have reported that account information and check information has been stolen this way.
- Hotel Safes - ITRC highly recommends that you lock up all valuables in room safes or hotel safes while you are out of your room. That includes laptops, PDA's, jewelry, passports, and other documents that contain personal identifying information or that would be of interest to a thief. A suitcase is not a secure way to lock up information.
- Pickpockets can be found in most major cities and tend to focus on high traffic areas that attract business or vacation travelers. Some studies indicate that wallets stolen in tourist spots frequently lead to identity theft. These professionals aren't interested in cash. They want your SSN, checks and driver's license.

Vacation travelers should use fanny packs or travel pouches that are worn inside your shirt to carry important documents.

Business travelers should be aware that pickpockets are also looking for laptops and PDA's that are temporarily out of your control- at airports, in lobbies and in dining areas.

- Wallets - Don't take anything in your wallet that is not absolutely necessary. Leave all cards with Social Security Numbers on them at home.
- Shoulder surfers - Besides pickpockets, identity thieves take advantage of people via shoulder surfing. "Shoulder Surfing" used to only apply to those who looked "over your shoulder" to see information. With the common use of cell phones, it is important to remember that you are in a public venue and may talk about things that a thief can use.
- Back-up material - carry photocopies of all travel documents including plane tickets, hotel reservations and passports. Keep these in a separate location from the originals.
- Mail - Put your mail on "postal hold" stating that for a period of time you wish to have your mail held at the post office. We prefer that term rather than "vacation hold" so that postal clerks will not know that you will be gone.

For the complete list of travel tips (and the accompanying check list), click here [Fact Sheet 122 Identity Theft Travel Tips](#)

Scam Alerts

ITRC 2008 Victim Survey

Identity Theft: The Aftermath 2008

The Aftermath – a portal into the world of identity theft victimization
By Linda Foley, ITRC Founder

For the past six years, the ITRC has conducted an annual survey about the feeling and experiences of identity theft victims we worked with. The first report was a follow-up on a survey done by PRC and CalPIRG. I know that from my experience as an identity theft victim, I was reluctant to explore my emotions and chronicle my journey as a victim. It hurt to relive those years and to let feelings I had denied rise to the surface. But I answered the questions in hope that life would change for those who followed.

Maybe my small voice might make a difference. And it did!

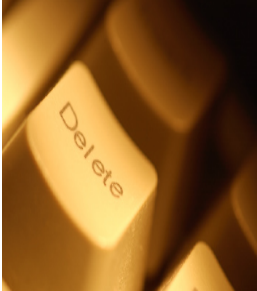
That early report got press attention and was quoted often in legislation. ITRC decided that it was important to continue that work, conduct yearly surveys and release annual reports about identity theft victimization.

Victims rarely had a public voice at legislative hearings or in the business community at conferences and workshops. Now, due to the efforts of many advocates and the information presented in *The Aftermath*, identity theft is not seen as a "victimless" crime. Our input is sought and we are encouraged to present the victim's perspective.

The Aftermath continues to serve as the voice of all identity theft victims: those who have been betrayed, misunderstood, considered guilty until proven innocent, and left wondering if life will ever be the same.

Job Scams

With the economy coming out of a recession slowly, and many Americans finding themselves without a job, it is important to remain vigilant of those who may try to take advantage of you. Job scams are becoming more and more prevalent as more Americans become desperate to find new ways to support themselves. There are many different variations of "job scams", but all of them will ultimately leave you in a worse situation than when you started.



Though the internet is a good place to search for job opportunities, it is important to be watchful of common scams. Free internet job postings are a hotbed for scam artists because they do not have to prove that they are indeed the company they say they are in order to place an ad. They will ask the applicant for personal information that could be used to steal their identity (such as Social Security Number, birth date, address, etc.) and then the applicant never hears from them again.

Another common scam is the "work from home" scam. For example, when the applicant is "paid" for receiving packages and sending them to another address. Or receiving checks in the mail and wiring a portion of the check to another location. Almost all of these will ask you to send the item to another country. Both are scams that could not only leave the victim in serious financial debt, but possibly charged for check fraud, money laundering, and/or receiving stolen goods.

It is vital to look for the signs that could indicate a possible scam. If they ask you to receive and send anything, it's most likely a scam. If they are asking for personal information before they meet you face-to-face in an office building, it is most likely a scam.

For more information on this type scam and how to stay safe, [click here](#).

The Romance of Identity Theft

My Name is Gladiator

Long before Social Security Numbers, driver's licenses, and the internet, there was something called a "diptych". According to Irulan Serena on [AllExperts.com](#), this small wooden birth certificate was issued in Ancient Rome as a means of identifying the holder as a Roman citizen. Diptychs made of bronze, silver and gold were given to those who ranked among the nobility.

Can you imagine what would happen if you lost your "wallet"? Forget about long lines at the Social Security office, you might find yourself in the lowest possible class of Roman citizenry. On the other hand, whoever "found" it would be sentenced to death as it would be assumed that anyone in false possession of a diptych had killed the original owner.

Throughout the centuries, one's identity could not be easily proven or disproven as there were no means of authenticating or verifying your word. As one traveled the world, there was no electronic database to confirm that you were who you said you were. No photo identification was available to support your claim.

The movie blockbuster *Gladiator* highlights this point. When Commodus demands that Maximus declare his identity "Why doesn't the hero reveal himself and tell us all your real name? You do have a name", Maximus replies "My name is Gladiator." In reality, he was

ITRC thanks the victims who participated in this survey and those in previous years. Others may not understand, but we opened a wound when we asked you to respond. ITRC will never let anyone forget what you've gone through. Your voice will make a difference and echo for years.

Click here for the [Aftermath 2008 Study](#)

For the Consumer

TrendWatch Widget

Trend Micro, through its Internet Safety for Kids & Families initiative and its commitment to making the Internet a safer place, recently announced its partnership with the ITRC. Both organizations recognize a need for increased consumer awareness and education on the best practices to prevent identity theft.

Trend Micro Announces Free Web Site Security Tool

Appearances can be deceiving – even "safe" or "respectable" Web sites can be dangerous if compromised by cyber-criminals. To help protect consumers from becoming victims of identity theft, Trend Micro is pleased to offer the new TrendWatch Widget, a free a Web site threat resource tool for consumers, IT staff, channel partners and anyone interested in receiving up-to-date information on the security of the Web. The widget provides current threat levels for Web, email and file; the latest Trend Micro malware blog entries; current security advisories (malware and vulnerabilities); and the ability to check the safety of a URL directly from the desktop by linking into the company's cloud-client infrastructure, the Trend Micro Smart Protection Network, to help identify and block threats before they have a chance to reach the desktop and infect.

This free tool can be easily downloaded

Maximus Decimus Meridius, commander of the Armies of the North, General of the Felix Legions, loyal servant to the true emperor, Marcus Aurelius...no proof needed.

Legislative Updates

New Mexico is the latest state to pass an ID Theft Passport law. It will go into effect on 7/1/2009.

Maine has recently updated its Security Breach Law mandating notification within 7 days, unless otherwise specified by law enforcement. It will become effective 90 days after 7/17/2009.

[Click here to subscribe](#)

Click [here](#) for Inaugural Issue of itr@c news

here: <http://go.trendmicro.com/widget/>
or check it out on the IIRC website:
<http://www.idtheftcenter.org/live-scam-news.shtml>.

My ID Score

Just as you would monitor your health status or your credit status, you should review your identity score to see if fraudsters may be misusing your personal information.

My ID Score is a great resource for consumers who are concerned about the unauthorized use of their identity. It is also a powerful and complementary tool for consumers affected by a data breach.

My ID Score is a quick and easy way to assess whether your personal information is being used fraudulently to obtain assets, goods or services in your good name. For those consumers who use My ID Score they can quickly determine whether or not they have been harmed as a result of a data breach or identity theft.

My ID Score is based on technology currently used by leading communications, financial services, retail companies, healthcare providers, government agencies, and consumers to assess their risk of identity fraud.

My ID Score is calculated using the ID Network® – the nation's only real-time, cross-industry compilation of identity information – to give consumers actionable insight into their risk of identity fraud. My ID Score is an excellent way to compliment more traditional identity theft prevention approaches such as credit monitoring, fraud alerts, and credit freezes.

Click here for MyIDScore.com

If you no longer wish to receive these emails, please reply to this message with "Unsubscribe" in the subject line or simply click on the following link: [Unsubscribe](#)

[Click here](#) to forward this email to a friend

Identity Theft Resource Center
P.O. Box 26833
San Diego, CA 92196
US

[Read](#) the VerticalResponse marketing policy.

