

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

Identity Theft Resource Center



ITRaC News - Q3 2009

A Message from the ITRC

The ITRC has always recognized that in identity theft there are at least two victims: the person whose personal information was used, and the business or agency that lost goods, services or money. The business losses are rarely counted as part of the identity theft equation, but this loss is an important part of the entire picture. The ITRC, as a victim advocate, believes that all victims should be considered if we wish to really understand the whole story on identity theft. Our work goes well beyond individual victims, and includes company breach mitigation and commercial (business) identity theft.

In a recent well publicized breach, over 100 million transactions were exposed, affecting more than 650 financial institutions. Many companies had to replace all the affected debit and credit cards at their own cost, as well as deal with the financial burden of any fraudulent purchases. The true number of "victims" (consumers and businesses) of this particular major breach is unknown, and may remain unknown, but is certainly huge. The quoted statistics don't tell the entire story, but rather only give us an indication of the size of the situation.

The questions these events should prompt are "what can we learn from the situation" and "how can we apply this knowledge to outwitting the thieves?" Vigilance and proactive efforts by both individuals and companies are required to meet this challenge. Computer and financial systems need ongoing testing for vulnerabilities, because that is **exactly what the thieves are doing**. We must approach identity theft as a team, and not permit individual concerns to outweigh the common good. Discord is precisely what the thieves want. Let's not cooperate.

Linda Foley, Founder, ITRC

Is Anyone Safe from Identity Theft



In This Issue

[Is Anyone Safe From Identity Theft?](#)
[Identity Theft and Employment](#)
[The Sandbox](#)
[Job Seekers Beware](#)
[Scam Alerts](#)
[For the Consumer](#)
[Legislative Updates](#)

**Protect Your
Identity Week**

Part III - Steps for the Consumer

It is important for consumers to be aware that their personal identifying information (PII) is vulnerable to exposure. Recognizing the numerous ways consumers can become victims of identity theft, many businesses have been established to assist consumers in "protecting" their identity. The last issue of ITRaC News newsletter addressed the no-charge (or minimal fee) methods by which consumers could take proactive measures to protect their PII. In this issue, we are covering the different fee-based products and services that are currently available to the consumer. Please understand that some of the following products and/or services are reactive in nature, providing notice of a problem after the fact.

Identity Theft Products Available

Many of the consumer products currently on the market sound enticing. The question each consumer must ask is "what do they cover?" If the product only monitors your credit reports, it will not tell you that someone skimmed your existing credit card at a restaurant and is buying bags of new clothes while you are at work. It also won't let you know that someone is receiving government benefits in your name.

It is important to educate yourself on identity theft and the "prevention" products available. This list includes: Credit Monitoring Services; Identity Monitoring Services; Credit Freeze Products; Data Sweep Services and Secure Payment Agents (SPAs) – see *For the Consumer* below. Other products include Victim Resolution services and Identity Theft Insurance. For the complete article, [click here](#).

As you consider these types of products, ITRC would like to remind you to shop carefully, read contracts and privacy policies, and check out companies with the Better Business Bureau or state Attorneys General. You can also do an Internet search for complaints about specific companies or services. There are many companies that are offering a combination of these services. Many of them are beneficial. However, it's your responsibility to understand the wide range of identity theft issues and determine the benefit of the services offered.

It's up to you to decide what product(s) fits your needs most. Personal activities like document shredding and keeping personal information secure do not eliminate the fact that you only control a limited amount of your personal information. Remember, there is no way to completely eliminate the chance of becoming an identity theft victim. However, with heightened awareness and proactive steps you can certainly reduce your risk dramatically.

For more detailed information on the types of products and services available, and suggested questions to ask, please refer to [ITRC Fact Sheet 132 Identity Theft Products](#)

Job Seekers Beware

The ITRC is proud to support the National Foundation for Credit Counseling (NFCC) and Council of Better Business Bureaus joint National Protect Your Identity Week (P.Y.I.W.) October 17-24, 2009.



During P.Y.I.W., hundreds of identity theft protection events will be held in communities across the nation. Additionally, many events will feature professional speakers and experts on ID theft prevention and recovery. A consumer Web site has been developed to highlight P.Y.I.W. events and provide valuable identity theft awareness and prevention education. The Web site, www.ProtectYourIDNow.org, features a map where consumers can locate events near them.

Identity Theft and Employment

"Financial identity theft" continues to be the most highly visible and publicized form of identity theft. As such, the other types of identity theft often go unnoticed. However, another type of identity theft is on the rise, what the ITRC categorizes as "governmental identity theft."

Obtaining employment, using another's personal identifying information and fraudulent documents, is just one type of governmental identity theft. (This type of identity theft also includes governmental services, benefits or IRS issues.) In 2008, about 15% of the 313,982 identity theft complaints reported to the FTC involved employment-related fraud (Consumer Sentinel Network Identity Theft Complaints, February 2009).

With today's high level of unemployment, more and more people are finding out they are not eligible for benefits because of identity theft issues, i.e. their benefits are already being issued to someone else or income from other jobs is being reported. Unfortunately it is left up to the victim, now unemployed, to try to mitigate their case before receiving their benefits. These types of cases are often quite complex and victims frequently need assistance from a victim advocate.

Fraudulent employment continues to be epidemic around the country. This is partly

Job Hunting Tips

With the unemployment rate rising and living costs going up, more people are looking for new jobs or second jobs. Job seekers often register with employment agencies, check employment ads, mail out unsolicited resumes, network with others, post resumes on job search sites, and often search craigslist. Unfortunately identity thieves are taking advantage of these uncertain economic times to scam job seekers and gather personal identifying information. The ITRC offers these suggestions:

Resumes and On-Line Applications:

- Never put your Social Security Number or Taxpayer ID number on a resume or application. Additionally, do not include driver's license number or professional license numbers. Most items of PII should be only provided during an interview, not on a job application.
- Omit home address and consider just using city and state.
- Consider opening a separate email account for your job search and keep your primary email address private. Placing your email address on a resume could open the door to spam and phishing, account verification, and other email scams.
- Do not provide such personal information as marital status or hobbies.

Internet and Newspaper Ads:

- Validate a company you find on a website carefully before giving them your information. Anyone can create a website, but it certainly doesn't mean that they are a real company. Most reputable companies will have a significant presence on the Internet.
- Confirm any and all contact information for the business. Does the email contain the domain name of the company? Is the FAX number in the same area code as the corporate number? Most importantly, does the company list a "brick and mortar" physical address that can be verified?
- Confirm the location of the company. Is it within the U.S.?
- Avoid any website that requires you to "pre-register" with your SSN, home address or driver's license number. Also, you should not be required to prepay to view job listings. The presence of these requirements are strong indicators of a scam.
- Update your computer security prior to emailing resumes and receiving email correspondence. Make sure your computer security is currently updated against viruses, trojans, and other types of computer malware. This can help to protect you from any intrusion or computer attack.

Background Screening:

- Companies might want to conduct a background check of you, both financial and/or criminal. Some people find out they are victims of identity theft during this process. Please be aware that you are allowed to view the results of any background checks, so that you can verify their accuracy.
- If you find an error in your report, let the interviewer know immediately. Ask for a photocopy of the report and tell them that this is either fraudulent or a clerical error. Ask for a few days to investigate the problem.
- If the error/fraudulent records are in your credit history, you automatically qualify for a free credit report from each of the credit reporting agencies. Call Equifax (800-525-6285), Experian (888-397-3742), and TransUnion (800-680-7289) to request your Credit Reports.
- If the error is in a criminal background check, you need to contact the law enforcement agency that reported the criminal incident, i.e. outstanding warrant, and find out what is going on. Please contact the ITRC if you need help with this process, toll free (888) 400-5530.

The safest ways to job search are to use local want ads, visit the unemployment office, use temp employment services, tell friends and family about your search, and network via professional groups and business acquaintances. When contacting a local company, you

caused by systemic problems due to the lack of authentication and verification. This growth is evidenced by the Social Security Administration's Earnings Suspense File which reflects an inordinate amount of misuse of Social Security numbers for employment purposes.

"Authentication" is the process of verifying that someone is who he or she claims to be. It is distinguished from "identification," which simply matches an individual with his or her records, but does not prove that the individual is who he or she purports to be.

Although the SSN generally is inadequate as a sole authenticator, it can be used effectively in the authentication process, i.e. used to attain background checks which can contain relevant and personal information about an individual to help verify an identity. (FTC Commission Report Dec 2008).

The Sandbox

"Muscles from Brussels to the Rescue"

By Josef Cannon

*Author, Actor, Law Maker & ITRC Video
Stolen Futures Narrator*

I never imagined the actor Jean-Claude Van Dame, known for his splits and spinning kicks, would be a prominent figure and major supporter of the recovery and return of my abducted daughter, Shelby Nicole Cannon. In addition, that he would become an outspoken advocate against identity theft.

Shelby was kidnapped and missing for more than eleven years, using a name and identity stolen from a graveyard tomb-stone in Ireland. Children have become prime targets for identity theft, as most individuals are not involved in credit transactions until (at the earliest) between the ages of fourteen to eighteen.

Child Identity Theft continues to be a growing trend for identity thieves as parents do not think to check their child's credit until they are looking to buy a car, apply for financial aid, or attempt to get a job that requires a background or credit check. Child Identity Theft can begin as early as infancy, leaving a possible decade or more of unmonitored criminal activity.

can physically meet them, see the facilities, and ask acquaintances in that industry about their reputation. It is very risky to contact foreign companies, especially those from Africa, Russia, and Asia, unless you have direct knowledge of their credibility.

For a more complete list of tips and suggestions, please refer to [ITRC Fact Sheet 121 Identity Theft Prevention Tips for Job Seekers](#)

Scam Alerts

Job Seekers Beware of Internet Scams

Job seekers need to be on the lookout for an ever-growing number of online scams targeting those who are looking for employment. "For many seeking work, the Internet has taken the place of local newspapers when focusing on job hunting efforts," says Jay Foley, ITRC Executive Director.

According to the [Internet Crime Complaint Center \(IC3\)](#), employment/ business opportunity schemes have surfaced wherein bogus foreign-based companies are recruiting citizens in the U.S. on several employment-search websites for work-at-home employment opportunities. Internet sites (i.e. Google, Craigslist and Twitter) have become hotbeds for these types of fraudulent job listings.

To avoid falling for some of these scams, [craigslist.org](#) suggests the following common-sense rules:

- **Deal locally with folks you can meet in person**
- Never wire funds via western Union, Moneygram or any other wire service
- Never give out financial information
- Avoid deals involving shipping or escrow services

In addition, the Better Business Bureau warns job hunters to look for the following warning signs (BBB, [Work-at-Home Schemes](#)):

- Overstated claims of product effectiveness
- Exaggerated claims of potential earnings, profits, or part-time earnings;
- Claims of "inside" information;
- Requirements of money for instructions or products before telling you how the plan works;
- Claims of "no experience necessary."

High profile entertainers, like Jean-Claude Van Damme, run the risk of rabid fans not just impersonating them but assuming their identities. This is evidenced in other celebrity cases like Paris Hilton (Socialite), Reuben Studdard (American Idol Winner) and Tiger Woods (Pro-Golfer) to name a few. It was the revelation that my daughter's abduction, (funded by monies collected through the usage of stolen identities), which sent the rugged action star into a compassionate and humanitarian mode.

After I landed a leading role opposite Jean-Claude Van Damme in the upcoming film *The Eagle Path*, Mr. Van Damme became familiar with my story. As he began to hear more about my daughter's abduction and identity theft, and my involvement with the ITRC and the Synclair-Cannon Child Abduction Prevention Act, the angrier, sadder, and more involved he became. In an attempt to bring this horrific crime to the spotlight, we decided to include Shelby in our recently completed film as the young child of my character. Our anticipated goal by including Shelby in the story/film, was to bring media attention to these widespread and detrimental issues of both identity theft and child abduction. We hope the publicity will encourage parents to take steps to protect their children and their identities.

As research shows, the majority of child identity theft is carefully crafted by parents, step-parents or family members closest to the child. In my case, the perpetrator had taken the time to develop an intricate and elaborate plan to abduct my daughter and take her to another country. She did this by canvassing old and abandon cemeteries & graveyards then stealing the identity of a child of a similar age who had recently passed away.

It was a miracle, the once in a lifetime encounter that many parents of missing children pray for but few attain, that led to her discovery. A reporter, (Nicola Tallant) in Ireland did a cover story on Shelby and I, along with actor Pierce Brosnan, who was attending the anniversary of the "Synclair-Cannon Child Abduction Prevention Act". This article appeared in an Irish newspaper which was spotted by a woman on vacation to Scotland while waiting in the airport. Upon seeing the photo of my daughter she recognized the face but the name/identity was different from the

For the Consumer

Secure Payment Agents (SPA)

The ITRC has long been concerned about the vulnerability of personal identity information (PII) on the Internet. Consumers regularly give up their credit/debit card information in online transactions. The ITRC and Internet experts recognize that the ideal solution to this problem would be to not transmit personal information to websites at all. The ability to shop, pay bills, or sign up at sites without ever giving out any personal information would represent a significant improvement in online safety standards.

ITRC recently identified an emerging category of proactive services and classified them as Secure Payment Agents (SPAs). A SPA is a method of protecting your personal information that allows you to remain completely anonymous while conducting online transactions or signing up at web sites - so you never give up your personal information.

The ITRC feels the introduction of this type of product will benefit consumers and businesses by dramatically reducing the amount of personal information required for many business and consumer Internet transactions.

ITRC has recognized Shop Shield® as the first product to meet the criteria and standards established for SPAs. [Click here](#) for the ITRC Consumer Awareness Survey and Secure Payment Agents White Paper.

Kemesa (Keeps Me Safe) is offering a free trial of Shop Shield® at no charge or obligation to ITRC visitors. For a limited time you will be able to sign up for the full array of the Shop Shield® services. To learn more about this offer and how Shop Shield® works go to the [Shop Shield](#) website.

35-Year Old Case of Identity Theft Solved

An Oregon man is so happy about the arrest of his imposter that he said he could kiss the special agent who handled it. The victim has known since the 1970's that his brother's friend stole his identity and had appealed for help from everyone for more than three decades. He even called the thief's mother to enlist her support.

Earlier this year an insurance fraud investigator, checking a bad claim made by the imposter, turned the case over to the OIG of SSA and an arrest was made.

Click here to read full [AP article](#)

Legislative Updates

Indiana Enacts House Enrolled Act No. 1121

Indiana recently enacted an identity theft bill that further enhanced law enforcement's ability to investigate and prosecute identity crimes and further enhanced victims' ability to recover from the crime. <http://www.indianaconsumer.com/idtheft/>

Effective July 1, 2009, House Enrolled Act 1121 does the following:

- Formally establishes the Identity Theft Unit
- Makes sythetic identity deception a crime [read more](#)
-

child she had known as a student in her son's class back in Liverpool England. This was my once in a lifetime break to finding my beloved daughter, Shelby.

My story wasn't the first of its kind - Jean-Claude Van Damme shocked me with his kind gesture to help in any way possible. The tears in his eyes, as we spoke about not only Shelby but the numerous amounts of children who are victims of Abduction and identity theft, were genuine and his actions support that. When many "Hollywood types" would use this moment to hype their own careers, Mr. Van Damme has kept quiet, yet his amazingly selfless act speaks volumes.

Josef's upcoming non-fiction book on the abduction and recovery of his daughter Shelby entitled "[Don't worry, Daddy's Coming](#)" will be released in fall of 2009.

Josef Cannon is the co-founder of CK [Cannon-Karst Productions](#) an entertainment company based in both London England & Marina Del Rey California with a focus on film, television and music.

Child Identity Theft

Adults are not the only targets of identity theft. Since children now have Social Security numbers within the first year of birth, they present an 18-year window of opportunity for thieves. Sometimes the perpetrator can even be one of the parents. Often kids don't find out until they turn 18 and start to apply for credit or loans.

There is information on the ITRC website, should you be concerned about child identity theft issues, [ITRC Fact Sheet 120B A Guide for Parents](#). More on this topic next issue.

If you are aware of someone who might be a victim, have them contact the ITRC for help.

ITRaC News [Q1 2009](#)

ITRaC News [Q2 2009](#)

Strengthens the penalty for stealing a child's identity [read more](#)

- Creates recovery tools for victims
- Enhances personal information security rules
- Prohibits sloppy or unfair business practices that can lead to identity theft.

[Click here](#) to read the full text of the bill

Missouri Enacts a Data Breach Notification Law

Missouri recently became the 45th state to require businesses holding certain personal information to provide notification in the event of a breach. Only Alabama, Kentucky, Mississippi, New Mexico, and South Dakota remain without such a law. While all of the state breach notification statutes are similar, they are not the same.

Like most data breach notification laws, Missouri's law requires businesses, as well as governmental agencies in Missouri, to notify state residents if their unencrypted or unredacted computerized personal information is breached. However, while the information triggering a breach in most states is limited to Social Security numbers, drivers' license or state identification numbers and financial account numbers, Missouri joins a handful of other states, including Arkansas, California, and Texas in requiring a notification where certain types of health data has been breached. ([Jackson / Lewis, August 13, 2009](#))

Missouri House Bill 62 is available at <http://www.house.mo.gov/billtracking/bills091/billpdf/truly/HB0062T.PDF>

[Click here to subscribe](#)

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
9672 Via Excelencia, #101
San Diego, California 92126
US

[Read](#) the VerticalResponse marketing policy.

