

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

Identity Theft Resource Center



ITRaC News - Q1 2010

A Message from the ITRC

Over the past year, the ITRC victim call center has noted a significant increase in the number of calls regarding Mortgage Fraud/Identity Theft. This trend seems to be supported by numbers released by the FBI. There were 67,190 Suspicious Activity Reports (SARs) referred to law enforcement during FY 2009, a six percent increase over FY 2008 ([see chart](#)).

Mortgage fraud is defined as a material misstatement, misrepresentation, or omissions relied upon by an underwriter or lender to fund, purchase, or insure a loan. Mortgage loan fraud is divided into two categories: fraud for property and fraud for profit. Fraud for property/housing entails misrepresentations by the applicant for the purpose of purchasing a property for a primary residence. Fraud for profit, however, often involves multiple loans and elaborate schemes perpetrated to gain illicit proceeds from property sales. (Source: FBI Financial Crimes Section, Financial Institution Fraud Unit, *Mortgage Fraud: A Guide for Investigators*, 2003) Many of these schemes involve industry insiders. Quite often accountants, mortgage brokers and lenders are involved in the schemes as they are familiar with the mortgage loan process and know how to exploit the vulnerabilities in the system.

As a result of the increase in the number of contacts regarding this type of financial identity theft, the ITRC developed [ITRC Solution 28 – Mortgage Fraud](#), to assist victims of this crime as well as to alert consumers of the need to take protective measures.

There are several entities which provide significant amounts of information on the topic of mortgage fraud. The FBI, which plays a major role in investigating mortgage fraud crimes, provides essential information on [How to Avoid Becoming a Victim](#) and maintains statistics on the prevalence of this crime. Another source of information on mortgage fraud issues is the [Freddie Mac](#) website. Freddie Mac's Fraud Investigation Unit (FIU) is responsible for the prevention, detection, investigation and resolution of mortgage



In This Issue

[The Sandbox](#)
[Mortgage Scams](#)
[Criminal Identity Theft](#)
[Scam Alerts](#)
[A Day in the Life](#)
[Dear Wilma](#)

What's Your Story?

Ready to tell your Internet safety story for the chance to win \$10,000

Create and upload a short original video in any style – serious confessional, educational PSA, or hilarious reenactment – showing what you've learned about the risks of, and ways to avoid, one of these Internet safety topics: identity theft, online scams & security risks; cyber-bullying and online predators; inappropriate content; and maintaining a good reputation online.

[Click here for details](#)

fraud. [Fannie Mae](#) is also committed to preventing mortgage fraud and offers resources to help detect and prevent mortgage fraud. [Financial Crimes Enforcement Network \(FinCEN\)](#), a bureau of the U.S. Department of the Treasury, provides a government-wide multisource financial intelligence and analysis network.

It is important for all property owners and consumers to be aware of this growing type of fraud. As long as the economy continues to be unstable, this type of crime will continue to threaten the financial health of our nation.

Mortgage Scams: FBI Warning May Protect Consumers Nationwide

Salt Lake City FBI and Utah Division of Real Estate Name Top Five Mortgage Scams in 2010

Special Agents and State Investigators Warn Consumers to Beware

- Is someone letting you live in a home for free?
- Did a builder offer you deep discounts to move into a newly constructed house?
- Has a company offered to refinance your mortgage for a fee?

If the answer to any of these questions is “yes,” then you may be a victim of a scam. FBI special agents and the state investigators with the Utah Division of Real Estate have compiled a list of top five mortgage related scams in 2010.

1. Reverse Mortgage Scam: Reverse mortgages can be a legitimate way for senior citizens to take equity from their homes without a monthly payment. However, con artists convince senior citizens they can live in a home for free, obtain a home loan under the occupant’s name, and disappear with the equity, leaving the victim to repay the mortgage.

2. Short Sale Fraud: A “short sale” transaction involves a lender agreeing to sell a property for less than the mortgage amount. Fraud occurs when a distressed homeowner finds a prospective buyer and they secretly set a low sale price. Unbeknownst to the lender, the buyer is willing to pay more for the property and the homeowner pockets the difference.

3. Builder Bailouts:

Simply put, builder bailouts are a “kick-back” scheme. They may be more common in a troubled real estate market where builders may have a surplus of unsold properties. The builder offers excessive “incentives” to the purchaser. These incentives are disclosed as a down payment which leads the lender to believe there is equity in a home. Under these circumstances the builder and the buyer are committing fraud.

4. Loan Modifications: The FBI Salt Lake City Field Office issued a consumer alert about loan modifications in the fall of 2009. Special agents and state investigators are concerned homeowners may fall for this same scam in 2010. Companies charge up to \$2000, promising to make a homeowner’s mortgage payment more affordable. But some homeowners report that they didn’t get what they paid for. For more information on loan modification scams

The Sandbox

High Tech Crimes

*by Brendan McHugh, DDA
San Diego County DA’s Office*

The Computer And Technology Crime High-Tech Response Team (CATCH) is a multi-agency task force formed in June 2000 to apprehend and prosecute all criminals who use technology to prey on the citizens of San Diego, Imperial, and Riverside Counties. CATCH believes that high-tech crime investigation requires information sharing and cooperation among all levels of government and without regard to traditional jurisdictional boundaries.

Consequently, CATCH was formed with law enforcement from three counties and combining local, state, and federal law enforcement agencies. CATCH also includes vertical prosecutors assigned from all jurisdictions in which it operates. This promotes the most thorough prosecution of the high-tech cases and provides for rapid communication between all levels of government.

CATCH recognizes that cooperation between it, other high-tech task forces, and the private sector industry is critical to the success of CATCH. With members including ESET, ITRC, SAIC, Sony, American Electronics Association, Cox Communications, UCSD and Qualcomm, CATCH has the support of a dynamic Steering Committee to assist CATCH in the assessment of crime risk and to prioritize high technology crime targets in the region.

Email account and social network profile take-overs are among the crime trends that the CATCH team has been investigating recently. These range from confidence schemes to harassment, and identity theft to

please find the 2009 news release at:

<http://saltlakecity.fbi.gov/pressrel/pressrel09/slc110409.htm>.

5. Affinity Fraud: Affinity fraud is an ongoing concern for the Salt Lake City FBI Field Office and the Utah Division of Real Estate. Fraudsters who promote affinity scams frequently are, or pretend to be, members of a particular religious, ethnic, or professional group. They often enlist respected community or religious leaders from within the group to spread the word about the scheme. They convince those people that a fraudulent investment is legitimate and worthwhile. Many times those leaders become unwitting victims of the fraudster's ruse.

For more crime tips or information on how to file a complaint with the FBI, please go to <http://fbi.gov/>.

Criminal Identity Theft

It's a terrifying scenario that occurs all too frequently. You're ready to buy a house or a new car, or start a new job. The prospect of taking this step is cause for both anxiety and excitement. After many months of planning or seeking that perfect opportunity, you're ready for that next big step in your life.

Then, the lender/salesman/banker/potential-employer returns with a pensive look on his face. He informs you that the job (or loan) you applied for cannot be approved. When you ask for the reason, they will hesitate, reluctant to inform you that a review of your background has revealed you have a criminal record!

"This has to be a mistake!" You may argue, you may protest, but in the final result the banker or merchant or employer will not determine the validity of the background check. He will only be able to proceed according to the information uncovered and company policy. You are denied. What you thought was going to be an exciting next step in your life has turned out to be the beginning of a severe challenge that, by the end, will cause significant stress, divert time and energy away from your other goals, and may even change your life forever. All the time and energy you will spend will not be used to advance yourself, but simply to attempt to repair what has been tarnished, your identity.

As someone who deals with victims of criminal identity theft every day, I have identified five of the most important tips I can think of to speed you along your road to recovery (see [Full Article](#)).

1. Don't act the victim. It means just what it says. When you find out that another has used your personal information without your consent to advance themselves at personal cost to you, it is completely natural to feel angry, betrayed, depressed, or overwhelmed. Try to control these emotions, and realize that you are the one that will have to assertively and proactively attack this problem in order for it to be resolved. There is no "cookie cutter" case in criminal identity theft. That also means there is no "cookie cutter" solution. Understand that only through your own determination can you fully resolve your criminal identity theft case.

2. Information is your best friend. The more you have, the better equipped you'll be, and the closer you are to resolution. The first

perpetrate fraud. One example of social engineering with an email account take-over is where suspects use a victim's contact list to send out false messages indicating that the victim has had some terrible misfortune and needs money sent to an account controlled by the suspect. The recipient anxious to assist who they believe is their friend in trouble, then unwittingly sends money to the suspect.

A relatively common example of online harassment is when a suspect takes over a victim's account and posts embarrassing or offensive content. Often this originates from a suspect the victim was previously intimate with. Once the relationship is over, the suspect takes over the victim's account, and posts nude or compromising photos of the victim with highly suggestive language, soliciting unwelcome contact.

Some of these take-overs are avoidable with a little diligence on the part of the account holders. By using complex passwords with a combination of special characters, upper and lower case letters, and numbers, it is much more difficult for a suspect to guess or crack the password. To preserve the account's integrity, it is important that one's account login and password not be shared with others. Some of the recent take-overs have been facilitated by devices such as key stroke loggers or by breaches to the hosting site(s). To minimize vulnerability to one of these methods, it is also important to periodically change one's passwords and maintain different passwords for different accounts.

Peer-to-peer (P2P) networks continue to be fertile ground for computer literate Identity Theft suspects. The users of peer to peer networks frequently mistakenly configure the shared drive options to share the entire contents of the drive. Often the investigations reveal that the file sharing program was

and most important thing you must do upon realizing you've become a victim of criminal identity theft is to get any and all information you can involving your case. In a criminal identity theft case, the beginning step is usually not as simple as picking up the phone and ordering a credit report. Somewhere, someone has committed some criminal offense using *your personal information*, whether it is the lowest traffic or parking violation, or as serious as a Class A Felony.

The best ally you can possibly have in a criminal identity theft case is someone willing to work with you to help you from within the law enforcement community. (See step 4) Once you know what jurisdiction the charges are coming from, you're well on your way to getting the situation resolved.

3. When working on your case, keep a detailed notebook of everything you do and everyone you talk to. If you're on the phone with a police agency who may give you instructions to go somewhere, call someone, or fill out some form - whatever that instruction or advice may be, *write it down*, along with the name and agency of whoever told it to you.

When you have to deal with multiple agencies or individual parties, you may get conflicting information or different advice depending on who you talk to. Knowing who said what to you will go a long way to establishing credibility with whoever you are talking to. Knowing they'll be held accountable to others for what they say to you will keep them strictly following agency/company guidelines, and not inventing their own. This is advantageous to you. As stated above, good information has now become your best friend. You want to hoard it like a bee collecting honey; you just can't have too much of it.

4. Find someone in law enforcement to believe in you. As a victim of criminal identity theft, you may find that those whose help you'll need in resolving your case may seem reluctant to help you. This is because, at first, *many will be unsure if you're truly the victim, or someone simply trying to avoid the responsibility of your actions.*

Unfortunately, because identity theft has really only been on the radar of law enforcement for the last ten years or so, many jurisdictions don't have much of a system for helping victims, or even a very good understanding of how serious a situation criminal identity theft can become. Everyone and I mean everyone - *will generally view the presence or lack thereof of a police report as the primary criteria for distinguishing the true victims from the possible criminals claiming innocence.* Without a police report, merchants won't remove fraudulent debts from your credit history, background check companies won't update your criminal history, and creditors will still view you as a liability. It is imperative you find someone in the law enforcement community that both believes you to be the victim that you say you are, and is willing to devote some of their busy work schedule to help you.

5. Above all and without exception, you must be totally honest and transparent in all your dealings related to your case. What you must understand is that, in-addition to any financial or legal difficulty your identity theft may have caused you, it is also going to cause you difficulty in a much less tangible yet potentially even more significant

downloaded and installed by children or grand-children on a computer used by the entire family. When the entire drive is shared, this allows perpetrators seeking personal finance, medical information, and employment information stored on the computer unfettered access to every file. For those who use P2P networks, the extent of the shared files and directories should be narrowly confined to items that are intended to be shared. A better practice, when practical, is to never store any personal information on a computer used in a P2P network. If children have access to a family computer, the responsible adults should monitor the computer use and routinely check for recently installed programs.

Victims of high tech crimes should understand that these crimes are very time sensitive. Frequently the information needed to identify a perpetrator must be tracked down immediately or it can be lost forever. Victims of high tech crimes should contact their local police agency and report the crime, and file a report online with the Internet Crime Complaint Center (IC3) at www.ic3.gov.

A Day in the Life of Victim Advisor

"I'm having a problem with Identity Theft!"

Just about every call starts like this. The problem is that since identity theft continually changes, most people don't know what it actually is or how to deal with the problems it has created. The victims I talk with are usually confused about how this could have happened to them. They feel a sense of paranoia because most don't have a direct idea of who the perpetrator might be. This also puts me in the position of having to gain their trust and that they can believe in the information I provide.

way. It's going to negatively impact the value of your good name, your *credibility*. If you are the true victim, you should never feel the need to be anything less than 100% honest. I don't care if you have a previous legitimate criminal history. If in the here and now, you're a victim, you still have the same rights as any other victim. Just be honest.

Even just the sense that you're not being 100% truthful will send those who may be willing to give you the benefit of the doubt running for the hills. Police officers will stop taking your phone calls; merchants will refuse to have their fraud people even review your claim; even lowly non-profit criminal investigators dedicated to identity theft will want to avoid you.

Criminal identity theft can be one of the scariest and most trying experiences a person may ever go through. Victims should find hope however in knowing that through educating yourself, being tenacious, and proactive in your pursuit of justice, it is something that can be resolved. The bottom line is, while assistance can be found, ultimately how you handle the situation will determine whether the final outcome is a positive or negative one. ITRC is here to help. Our toll-free line is 888-400-5530.

By Matt Davis, Criminal Identity Theft Advisor

Scam Alerts - Census Bureau

Fraudulent Activity and Scams

The Census Bureau uses a workforce of trained federal employees to conduct a variety of household and business surveys by telephone, in-person interviews, through the mail, and in limited cases through the Internet. We understand your personal information is sensitive, and go to great lengths to protect the data we collect. Although we cannot stop or warn against all bogus or false collections of data -- here are some tips to help you recognize fraudulent activity or unofficial data collections. If you are contacted for any of the following reasons -- Do Not Participate. It is NOT the U.S. Census Bureau

Phishing:

'Phishing' is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords, social security numbers, bank account or credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email and it often directs users to enter sensitive information at a fake web site whose look and feel are almost identical to the legitimate one.

Other Scams:

- The Census Bureau does NOT conduct the 2010 Census via the Internet
- The Census Bureau does not send emails about participating in the 2010 Census
- The Census Bureau never:
 - Asks for your full social security number
 - Asks for money or a donation
 - Sends requests on behalf of a political party

If the victim is willing to work with me and not take shortcuts or stop mid-stream, I know we can resolve the case. It's a hard part of the job to understand that some victims stall out. However, once I had some experience helping victims, I could easily tell who was and who wasn't going to follow through. Most I can educate and encourage to complete the mitigation before things progress. Others end up calling me several months later upset that things have gotten worse. Then we have to start again - with the understanding that they have to complete the process to resolve the case.

Another difficult aspect of the job is you have to be prepared for anything. Sometimes it may be as easy as canceling a credit card, placing a fraud alert and checking your credit reports. However, it can also be difficult and heart breaking such as when you hear from a teenager applying for a college loan only to find out that a family member has been using their SSN for years. It will mean getting that loan and attending school is going to be delayed by a semester at best. Child and family identity theft is hard on everyone since emotions enter at each decision point.

When my phone rings I don't know what to expect on the other side of the receiver. It kind of makes me think of the movie *Forest Gump* (italicize). "Life is like a box of chocolates; you never know what your going to get." But at the end of the day, no matter how stressful, I always feel good that I'm helping people.

Brendan, ITRC Victim Advisor

Dear Wilma

Dear Wilma,
I met this girl on an online dating site. I think we are falling in love. She doesn't live in America and I am going to go visit her in Nigeria. She said it is best to send her



- Requests PIN codes, passwords or similar access information for credit cards, banks or other financial accounts.

How to report scams and bogus Census web sites

If you believe you have been contacted as part of bogus or fraudulent activity falsely representing the Census Bureau:

- In Person Scam
 - Check for a valid Census ID badge
 - Call your [regional office](#) to verify you are in a survey
- Email Scams
 - If you think it is a bogus email, do not reply or click on any links within the email.
 - Do not open any attachments. Attachments may contain code that could infect your computer
 - Forward the email or web site URL to the Census Bureau at ITSO.Fraud.Reporting@census.gov.
 - After you forward the email to us, delete the message. You will not receive a confirmation email after forwarding the information to us. However, the Census Bureau will investigate the information and notify you of its findings.
- Mail Scams
 - Contact the [United States Postal Inspection Service](#)



Is your survey legitimate?

You may further verify if a collection activity is legitimate by calling your [regional census office](#) regarding mail surveys, and our [National Processing Center](#) for phone surveys.

Other questions may be answered through our [Are You In a Survey?](#) page.

ITRaC News Q1 2009
ITRaC News Q2 2009
ITRaC News Q3 2009
ITRaC News Q4 2009

Toll-Free Victim Assistance
888-400-5530

\$500 before I come so that when I get there, she will have my spending money converted into local money. I totally trust her but my cousin says this is a scam. How do I know?

Sincerely,
Lovestuck Jim

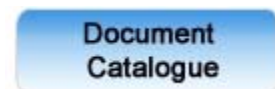
Jim,
You may have found love online, but if this person is asking for money; do not send it. You are being scammed. If you want to find love, go to church! Lots of single women there, or ask your friends to set you up with any single women they know. (Everybody has single friends)

Hate to tell you, but you may have fallen in love with a guy pretending to be a gal. Not the girl of your deams; but some fat guy sitting at a computer hoping to get some of your hard earned money.

So, do me this favor and stay off the computer when looking for love. A fool is soon parted from his money!

Love is out there. Good luck.
Wilma

ITRC New Hot Link



Find the ITRC on:



[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](#)

Identity Theft Resource Center
9672 Via Excelencia, #101
San Diego, California 92126
US



[Read](#) the VerticalResponse marketing policy.