



**SPECIAL REPORT**

**Avoiding Internet Scams**

**And Identity Theft**

**ROSENBERG FINANCIAL GROUP, INC.**

Identity Theft is a very large problem. It's hard to find an accurate number of Americans who have been affected by identity theft, but most estimates are over 10 million people. Even the IRS got scammed. In August, 2012, they determined that they may have delivered as much as \$5 billion in checks to identity thieves. And they estimated that number could grow to \$21 billion over the next five years. (source: [www.cnbc.com](http://www.cnbc.com)). This is a very serious matter.

But identity theft is only one way that people lose lots of money to scammers. Internet dating scams, Ponzi schemes, forgery, theft by family members and similar deeds are other ways people lose their money. Unfortunately, many of these losses could have been avoided if the victims had just taken some very simple steps and used some common sense to protect themselves

How do identity thieves get information about you? Here are just a few things they might do. We will discuss some of them as we go forward.

- Go through trash cans and dumpsters, stealing bills and documents that contain personal information.
- Work for businesses, medical offices, or government agencies, and steal personal information on the job.
- Misuse the name of a legitimate business, and call or send emails that trick you into revealing personal information.
- Pretend to offer a job, a loan, or an apartment, and ask you to send personal information to "qualify."
- Steal your wallet, purse, backpack, or mail, and remove your credit cards, driver's license, passport, health insurance card, and other items that show personal information.
- Make you think you have won something and hope you respond.

### **10 Red Flags of Identity Theft**

- Mistakes on your bank, credit card, or other account statements
- Mistakes on the explanation of medical benefits from your health plan
- Your regular bills and account statements don't arrive on time
- Bills or collection notices for products or services you never received
- Calls from debt collectors about debts that don't belong to you
- A notice from the IRS that someone used your Social Security number
- Mail, email, or calls about accounts or jobs in your minor child's name
- Unwarranted collection notices on your credit report
- Businesses turn down your checks
- You are turned down unexpectedly for a loan or job

## **A Very Sad, But Very True, Story**

A very nice lady thought she had found love on the internet. Now, this is not unusual – it happens every day. But the problem is that matchmaking websites can easily be breeding grounds for scams. They make it very easy for anyone, from anywhere in the world, to create a profile and upload photos. There is absolutely no verification that the person is who they say they are.

The scammer told her a story that sounded good to her. He was supposedly from the local area, but was never in town. But they talked more and more on the phone, she started to believe that they were in a relationship.

He told her about an "investment" in a foreign country that would "make her a lot of money." He started talking to her about investing some money. He sounded very nice and she saw no reason not to believe him. Actually, she wanted to believe him. But as his story got bigger, so did her investment.

Now logic would tell you that she should have been suspicious. But all logic can go out the door when romance or the idea of making a lot of money is involved.

She was advised to speak with the Consumer Protection Agency in Atlanta, which she did. The people at the agency deal with international crime, so they are aware of scam artists all over the world who create fake profiles on internet dating sites. They explained to her that scammers post a photo of a model and create an appealing profile that will attract connections. Once a relationship begins, they start asking for money.

At the end of several months, she had taken the equity out of her home and wiped out her retirement accounts. On top of that, she still owes taxes on the money she withdrew. She told this story on *WMAZ Eyewitness News*.

How can this happen? Scammers know how to gain our trust, and our pity, and mentally catch us off-guard. They target people who may be lonely and looking for companionship. According to the Internet Crime Complaint Center, internet romance scams cost victims \$1 billion in 2015.

The purpose of this story isn't to reflect poorly on the victim. It's to let you know, as you read this report, what can happen if you're not careful.

## **Spotting Medical Identity Theft**

You don't hear much about it, but medical identity theft has become the fastest growing type of identity theft. According to the American Medical Association ([www.ama-assn.org](http://www.ama-assn.org)), an estimated 2 million people become victims each year. Medical identity theft occurs when someone uses another person's name or insurance information to get medical treatment, prescription drugs, or surgery. It also happens when dishonest people working in healthcare provider offices use another person's information to submit false bills to insurance companies.

How do you know if you've become a victim of medical identity theft? Here are some warning signs from the Federal Trade Commission ([www.ftc.org](http://www.ftc.org)):

- You get a bill for medical services you didn't receive
- You are contacted by a debt collector about medical bills you don't owe
- You see medical collection notices on your credit report that you don't recognize
- You find erroneous listings of office visits or treatments on your Explanation of Benefits (EOB)
- You are told by your health provider or insurance company that you have reached your limit of benefits

In addition to the obvious problems that medical identity theft creates, you also run the risk of receiving improper medical treatment because someone else's information is in your medical records.

How do you protect yourself? Here are a few things you can do:

- Check your Explanation of Benefits form and make sure that the information is correct. If not, then contact the provider and the insurance company or Medicare immediately.
- Don't give out personal or medical information over the phone unless you've initiated the contact.

- Beware of “free” health services or products from firms who require that you give them your health plan identification number.
- Remember that people might pose as employees of your healthcare providers or insurance companies. If you receive a call, and it sounds fishy, tell them you will call them back.
- Periodically check your credit reports to make sure there are no indications of medical identity theft or any other identity theft.

## The Top 10 Identity Theft Scams

It's interesting that most Identity Theft occurs because the victims cooperate with the perpetrators. Not on purpose, of course. They just get careless. So let's look at some of the more prominent online scams (www.business-time.com).

- **Phishing.** This is where people contact you to “fish” for your personal information. It occurs when you receive an email that looks like it's from your bank, your credit card provider, or your utility company. They will say there's a problem with your account and ask that you click on a link that will purportedly take you to the company's website. But, in reality, it takes you to a fake version of your company's site that asks you to enter your user name and password. First of all realize that your bank isn't going to send you any emails requesting that you go to their website. But if you are concerned, just call the bank and tell them what you received. One other very important fact. Emails will usually include highlighted links (called “hyperlinks”) that the scammers want you to click on. That link will take you to the bogus site *if you just put your cursor over that link, and then look at the bottom of your screen on the left hand side, you will see where that link would really take you.* And it won't be your bank. So you know it's a scam.
- **Texting.** This is also called “Smishing.” There's a term for everything! This occurs when you receive a text stating that you've won a prize. If you click on the link, it downloads malware. Don't click on any links that you may think are suspicious. Especially if they are offering something that is too good to be true. You can safely assume it's a scam.
- **Fake Job Offers.** This one targets anyone looking for work. You receive an e-mail pitch and the employer website looks real. They even hold a telephone interview and offer you a job. But wait, first they want you to complete an online credit form. Don't do it! By completing the form you will give them all the information they need to steal your identity.
- **Refinance Your Home.** A friend called last year for some advice. She had been thinking of refinancing her house and wanted my opinion on something she had just done. She went online to look for re-fi deals, and soon began receiving e-mails from companies offering very low rates. On the day she called me, she had received an e-mail that sounded really good. So she entered all of her personal information, and even pre-paid for the home inspection by credit card! When she told me this, I told her this could very well be a scam, and to call and ask for her money back immediately. I encouraged her to not respond to e-mails that came to her, since she really had no idea who sent them.
- **Facebook Users.** These scams target people using social networking sites. You see on your Facebook page that you've won a sweepstakes prize. Now all you have to do is click on the link. Don't do it! By clicking on the link you will give the scammers access to your personal information. In addition, by posting such facts as your birthday, where you went to school, when you graduated, etc., scammers can easily gather more information about you that you really don't want them to know.
- **Other Social Media.** These use actions and events to get your attention. You see a link that tells you to “click here” to watch a video, and when you click on the link a window pops up saying you need to first upgrade your Flash player. Don't do it! When you click on the download link, instead of getting a Flash upgrade you'll get a virus that finds your passwords.
- **Electronic Banking or Online Bill Pay.** You receive an e-mail that your recent financial transaction was unable to be processed, and they need additional information from you....Don't do it! The link they send you connects you to a fake bank web page that steals your information.

- **Online Bidding.** Targets anyone looking for a bargain. The website says you can win an iPad, a new computer, or a camera, all for just pennies a bid. Don't do it! You end up paying for every bid, even if you don't get the merchandise.
- **I'm Stranded.** One day I got an email from an acquaintance that said he was stranded in Europe and needed some money wired to him. It came from his e-mail address, and it looked totally logical. But I have trained myself to question every single e-mail that I receive. Even if I "know" the sender. So I thought about it, and it just didn't make sense. It was sent to a bunch of people in his address book, including people he didn't know well enough to ask for money. Although the email was written in English, I could tell it wasn't written by an American. On top of that, it just wasn't the way he spoke. I called him to let him know his account had been hacked. He had received several other calls and was taking action. Thankfully, nobody fell for this scheme.
- **IRS Wants More Information.** In early 2012 there was a run of emails supposedly from the IRS. It had the IRS logo and the IRS email address ([www.irs.gov](http://www.irs.gov)). But .... if you put your cursor over the link in the email, it would take you to a site someplace in France.

Play it safe. All of these activities, which are called phishing or spoofing, have the same thing in common: they are trying to get you to give them your personal information: bank account numbers, Social Security numbers, passwords, credit card numbers, etc.

So here's the rule: never, never, never respond to these emails. This is a situation where you want to shoot first and ask questions later. Assume that every email you get requesting information is a scam. Period. Just assume they're guilty and stay away. Don't click just to see what it is. Don't click to see how much money you've won. Just Don't Click! That'll save you a lot of money and aggravation.

The Internet Crime Complaint Center website (<http://www.ic3.gov/>) provides information about many scams. You can also submit a complaint if you have been a victim of an internet scam.

## Lock Down Your Credit

According to consumer advocate and tv/radio personality Clark Howard, *"When it comes to full-blown identity theft, only by doing a credit freeze can you protect yourself from the havoc a criminal may cause by opening new lines of credit in your name. A credit freeze costs anywhere from free to \$10 per bureau depending on your state. And that makes it the cheapest insurance you can buy against identity theft."* ([www.clarkhoward.com](http://www.clarkhoward.com))

While there are companies trying to scare people into paying for identity theft protection service, Clark says you can do it yourself for a fraction of the cost. That's because one of the techniques that identity theft protection companies use to prevent ID theft is to freeze your credit report.

On August 1, 2008, a credit freeze bill went into effect that provides Georgia consumers with the ability to place a freeze on their credit file for only \$3, or a total of \$9 for each of the three major credit-reporting agencies: Equifax, Experian and TransUnion. The freeze is free for senior citizens 65 and older and for victims of identity theft. Each temporary lift of the freeze - commonly called a thaw - to allow access to the consumer's credit file would also cost \$3. When you request a thaw, it should be available electronically within 15 minutes of request by the consumer, keeping on-the-spot credit an option for shoppers.

When a freeze is in place, credit reporting agencies may not release the consumer's credit file unless the consumer first removes the freeze by providing the consumer's password to the credit agency used by the merchant. Most lenders and creditors rely on access to a consumer's credit file to determine a consumer's credit worthiness. By denying such access, a credit freeze makes it very difficult for an identity thief to open a credit account or loan in a victim's name.

To place a credit freeze on your file, you must contact the credit reporting agencies at the addresses below:

- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348  
Online: <https://www.freeze.equifax.com/>

- Experian Security Freeze, P O Box 9554, Allen, TX 75013  
Online: <https://www.experian.com/freeze>
- TransUnion Security Freeze, P O Box 6791. Fullerton, CA 92834  
Online: <https://freeze.transunion.com>

Written requests must contain the following:

- Full name (and former name if applicable)
- Current Address and former address if it changed in the last 5 years
- Social Security number
- Date of birth
- Photocopy of a driver's license, state ID card or other government-issued identification
- Proof of current residence, such as a copy of a phone or utility bill.
- If you are a victim of identity theft, include a copy of either the police report; investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not 65 years of age or older or a victim of identity theft, include payment by check, money order or credit card (Visa, Master Card, American Express, or Discover cards only). Do not send cash in the mail. Read more about this law by visiting the Georgia Attorney General's website: <http://law.ga.gov/placing-credit-freeze-your-credit-report>

## **Do Not Call Me!**

In addition to being highly annoying, sales calls can be very dangerous. It could be someone just trying to get your personal information. But it's just not sales calls that can be dangerous, it's calls from people who have bad motives.

So here's a simple rule: if you ever receive a phone call, and the person tells you they are from the IRS, Social Security or Medicare, ask for their number and tell them you need to call them back later. Don't worry, they're not going to give you a number, because they are not with any of these agencies. But if they do give you a number, still don't call them back.

I received two calls earlier this year from a person who said he was with my cell phone company, and he said, "We are having some computer problems so I need to update your personal information." He knew my name, and called me on my cell phone, which momentarily caught me off guard. When he asked for the last four digits of my Social Security number, I knew this was a scam.

In addition, scammers have been making phone calls claiming to represent the National Do Not Call Registry. The calls claim to provide an opportunity to sign up for the Registry. These calls are not coming from the Registry or the Federal Trade Commission, and you should not respond to these calls.

Finally, we've heard reports of people who have received calls from people purporting to be with Microsoft. They are told that there's a virus on their computer and they need to go to a specific site and enter some personal information. Then they are asked for their credit card number.

Obviously, this is not going to be stopped by you being on the do not call list. Therefore, you must be diligent in your efforts and not give out any personal information to anyone you don't know.

To add your number to the Registry you can call 888-382-1222 or go online at <https://www.donotcall.gov>. Then click on "Register a Phone Number" in the left column of the page. You can register home and cell numbers.

Understand that your registration will not expire. Telephone numbers placed on the National Do Not Call Registry will remain on it permanently.

## Check Your Credit Reports For Free

In addition to not having to pay for identity theft protection, you also don't have to pay for credit reports. As a Georgia resident, you are entitled to 2 free credit reports each year from each of the three credit reporting agencies. That works out to a free credit report every other month.

This is why you should not go to <http://www.freecreditreport.com>. This is a commercial company that is trying to sell a credit protection plan.

Instead, you should go to: <http://www.annualcreditreport.com>. This is the one that is truly free. You need to review all of your credit reports since you are the only person who can tell if they are accurate. If you find errors, dispute them with the credit bureaus.

## If Your Identity is Stolen...

### 1. Flag Your Credit Reports

Call one of the nationwide credit reporting companies, and ask for a fraud alert on your credit report. The company you call must contact the other two so they can put fraud alerts on your files. An initial fraud alert is good for 90 days.

Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

The purpose of a fraud alert is for creditors to confirm that the person using your name is actually you. With your fraud alerts in place, creditors, lenders, or other prospective users of your consumer report must take steps to verify your identity before they can:

- Issue new credit
- Increase credit lines
- Arrange loans
- Create new accounts for such things as utilities and cellular phones

You may place a fraud alert on your credit report if you have a good faith suspicion that you have been or about to become a victim of identity theft. After a fraud alert has been placed in your credit file, any creditor using that credit file to grant new credit or an extension of credit in your name should take reasonable steps to verify your identity and confirm the credit application is not the result of identity theft. This can be done by contacting you by phone, via the mail or by using other methods to verify the application is legitimate. Most of the time, when someone else is trying to use your identity to get credit, the fraud alert will stop them cold.

### 2. Order Your Credit Reports

Each company's credit report about you is slightly different, so order a report from each company. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact the credit reporting company.

### 3. Create an Identity Theft Report

An Identity Theft Report can help you get fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name. To create an Identity Theft Report, go to [www.ftc.gov/complaint](http://www.ftc.gov/complaint) or call 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit

Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report. These two documents comprise an Identity Theft Report.

## What Does Rosenberg Financial Group, Inc. Do?

We believe that most investors want a specialist. They want to call and talk to a person that understands them and can provide for their needs. They don't want a person who represents a company that is trying to push more of their products through their sales system.

At Rosenberg Financial Group, Inc., we have created the **RetireRelax Solution™** that assists us in managing our clients' money. This disciplined investment approach for retirees and pre-retirees includes an exit strategy when we feel that risk is high. Keeping an eye on the investment landscape for our clients is something we do each and every day.

To learn more about us, just download the report: "**What Do I Need To Know About Rosenberg Financial Group, Inc.?**" from our website.

To learn about our complementary consultations, just download the report: "**What Can You Expect When You Come In For Your Complementary Consultation?**" from our website.

### Additional Free Reports On Our Website

- Can I Afford to Retire?
- Maximizing My Social Security Benefits
- What Do I Need To Do To Plan For My Secure Retirement?
- Who Will Really Get My Money When I Die?
- Your Stock Market Survival Guide
- Avoiding Internet Scams and Identity Theft
- Should I Keep My Money Where It Is Or Roll It Into An IRA?
- What To Do When Your Spouse Dies

If you would rather get paper reports, just call **844-337-3767** and leave a message as to which report(s) you are interested in. We'll mail them to you at no cost or obligation.

[www.RetireRelax.com](http://www.RetireRelax.com)

Be sure to listen to "Your Money" with Steve Rosenberg, Sherri Goss, and Randy Goss live every Saturday morning at 9:00 on WMAC, AM940. Sherri also appears as WMAZ's Financial Expert every Wednesday afternoon on the 5:00 edition of *Eyewitness News*. After her appearance, Sherri remains at the station until 6:00 and takes personal questions by phone off-the-air



**2517 Moody Road, Suite 100 · Warner Robins, GA 31088 · (478) 922-8100 · (800) 777-0867**

**4875 Riverside Drive, Suite 201 · Macon, GA 31210 · (478) 741-4457 · (800) 777-0867**

**Securities and Advisory Services Offered Through Royal Alliance Associates, Inc. Member FINRA/SIPC  
Advisory Services Offered Through Rosenberg Financial Group, Inc.,  
An Independent Registered Investment Advisor Not Affiliated With Royal Alliance Associates, Inc.**

The information herein has been obtained from sources we believe to be reliable, but we do not guarantee its accuracy or completeness. Neither the information nor any opinion expressed constitutes a solicitation for the purchase or sale of any security. Past performance is no guarantee of future results. Investing involves risk, including the potential loss of principal. No investment strategy can guarantee a profit or protect against loss in periods of declining values.

This is for informational purposes only and is not intended to be legal or tax recommendations, advice, or endorsements. Tax laws are complex and you should consult your tax advisor to find out how this information may apply to your specific situation. Please consult your tax advisor before making any decision that may affect your tax situation.

Websites provided in this paper are provided strictly as a courtesy. When you link to any of the websites provided herewith, neither Rosenberg Financial Group, Inc. nor Royal Alliance Associates, Inc. make any representation as to the completeness or accuracy of information provided at the sites.