TIPS

to avoid becoming a victim of fraud

If your Social Security card, personal, financial, or account information is lost or stolen, contact the credit reporting agencies and place a fraud alert on your credit file. Check your bank and other account statements for unusual activity. You may want to take additional steps, depending on what information was lost or stolen.

If your information is lost in a data breach, the organization that lost your information will notify you and tell you about your rights. Generally, you may choose to:

• **Monitor your accounts for unusual activity.** You have the right to obtain documents relating to fraudulent transactions made or accounts opened using your personal information. A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, if you ask for them in writing. A business may ask you for proof of your identity, a police report, and an affidavit before giving you the documents. If you ask, a debt collector must provide you with certain information about the debt you believe was incurred in your name by an identity thief.

• **Exercise your right to a free credit report.** Get a report from one of the bureaus every four months and look for anything suspicious. Use this site: **https://www.annualcreditreport.com.**

If you believe information in your file results from identity theft, you have the right to ask that a consumer reporting agency block that information from your file. You must identify the information to block, and provide the consumer reporting agency with proof of your identity and a copy of your identity theft report. The consumer reporting agency can refuse or cancel your request for a block if you don't provide the necessary documentation, or an error or a material misrepresentation of fact made by you. If the agency declines or rescinds the block, it must notify you.

• **Place a fraud alert on your credit file**. An initial fraud alert stays in your file for at least 90 days, it also entitles you to a copy of all the information at each of the three nationwide agencies. An extended alert entitles you to two free file disclosures in a 12-month period following the alert. If you believe it has inaccurate information due to fraud, such as identity theft.

Go to www.consumerfinance.gov/learnmore

Important Resouces

Equifax: (800) 525-6285
www.equifax.com

Experian: (888) 397-3742
www.experian.com

TransUnion: (800) 680-7289
www.transunion.com

Free Yearly Credit Report
www.annualcreditreport.com

Federal Trade Commission Hotline
www.identitytheft.gov
(877) 438-4338

Florida Attorney General Website
www.myfloridalegal.com

National Crime Prevention Council
www.ncpc.org

Consumer's Union
www.consumersunion.org

U.S. Department of Justice
www.justice.gov/criminal-fraud

AARP
www.aarp.org/idtheft

Florida's Hotline for Fraud
(866) 966-7226

Florida Residents
Request your free IRS PIN code to avoid ID theft.

Internal Revenue Service Assistance
www.irs.gov/individuals/get-an-identity-protection-pin
If you've paid your taxes and are getting calls:
(800) 366-4484
Forward phishing emails to: phishing@irs.gov

For more information, please contact
Bal Harbour Police Department
9700 Collins Avenue # 280
Bal Harbour Florida 33154
(305) 866-5000 - 24 HR Complaint Desk
(305) 866-4885 Fax

Edward Byrne
Memorial Justice Assistance Grant

Sources
www.irs.gov
www.ftc.gov

Bal Harbour Police Department

Mark Nathan Overton
Chief of Police

Reminds You

Don't Become Victim of

FRAUD

Identity Theft

Approximately 18.9 million people became the victims of identity theft in 2015, according to a report from the Department of Justice. Identity theft happens when someone steals your personal information and uses it without your permission. It's a serious crime that can wreak havoc with your finances, credit history, and reputation.

How can I tell if my information has been stolen?

• **Bills for goods or services you didn't purchase appear on your credit/debit card statements:** Don't ignore small charges. Crooks who buy stolen account numbers will sometimes do a test with a small purchase.

•**Statements show up for an unknown credit card account:** Thieves will use your information to open accounts then go on a shopping spree.

•**A new credit card or store charge card that you didn't apply for shows up in the mail**: An ID thief pretending to be you may have applied for that card. Don't assume it's a mistake. Contact the company right away.

•**Collection notices or calls for a debt you don't owe**: It could be an honest mistake; but It could be that an ID thief is using your personal information to buy things and not pay the bill. You'd better find out.

•**Errors (misinformation) on credit report**: You have the right to a free report every 12 months from the big three credit bureaus (Experian, Equifax and TransUnion).

•**You have good credit, but an application for credit is denied**: Don't get upset, find out what's going on. An identity thief could have mucked-up your credit file and ruined your credit score.

•**Missing mail or e-mail**: There could be a problem if the monthly statement from your bank or credit card company suddenly stops. A thief may have filed a change of address form to get that statement and keep you from spotting his dirty work for as long as possible.

• **Medical Providers** If you receive a bill you for services you didn't use or your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.

• **You get notice that your information was compromised by a data breach at a company** where you do business or have an account.

• **You are arrested** for a crime someone else allegedly committed in your name.

IRS Tax Related Scams

Tax Refund Scam Artists Posing as Taxpayer Advocacy Panel: Taxpayers are receiving emails that appear to be about a tax refund. These emails are a phishing scam, where unsolicited emails which seem to come from legitimate organizations but in reality are from scammers, trying to trick unsuspecting victims into providing personal and financial information. Do not respond or click any links.

IRS-Impersonation Telephone Scam: These are aggressive and threatening phone calls. Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting. Victims may be told they have a refund due to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an "urgent" callback request.

E-mail, Phishing and Malware Schemes: These emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. When people click on email links, they are taken to sites imitating an official-looking website, such as IRS.gov. The sites ask for personal information. These sites may also carry malware which allow criminals to access your files or track your keystrokes to gain information.

Note that the IRS will never:

1) call to demand immediate payment, nor will the agency call about taxes owed without first having mailed you a bill;

2) demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe;

3) require you to use a specific payment method for your taxes, such as a prepaid debit card;

4) ask for credit or debit card numbers over the phone;

5) threaten to bring in local police or other law enforcement groups to have you arrested for not paying.

Don't fall victim to tax scams. Remember, the IRS will ONLY contact you by mail

Phone Scams

Often, scammers who operate by phone don't want to give you time to think about their pitch; they just want you to say "yes." But some are so cunning that, even if you ask for more information, they seem happy to comply. They may direct you to a website or otherwise send information featuring "satisfied customers."

Here are a few red flags to help you spot telemarketing scams. If you hear a line that sounds like this, say "no, thank you," then, hang up.

•You've been specially selected (for this offer).
• You'll get a free bonus if you buy our product.
• You've won one of five valuable prizes.
• You've won big money in a foreign lottery.
• This investment is low risk and provides a higher return than you can get anywhere else.
• You have to make up your mind right away.
• "This is not a telemarketer call"
• We'll just put the shipping and handling charges on your credit card.

How They Hook You

Scammers use exaggerated or even fake prizes, products or services as bait. Here are a few examples of "offers" you might get:

• **Microsoft Scam**: Scammers might call you on the telephone and claim to be from Microsoft. They might offer to help solve computer problems or sell you a software license. Microsoft does not make unsolicited phone calls.
• **Packages**: "Free" or "low cost" vacations .
• **Credit and loans**: Advance fee loans, payday loans, credit card protection, and offers to lower your credit card interest rates.
• **Sham or exaggerated business and investment opportunities**: Promoters of these have made millions of dollars.
• **Charitable causes**: Urgent requests for recent disaster relief efforts,especially over on the phone.
• **High-stakes foreign lotteries**: These pitches are against the law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.
• **Extended car warranties:** Scammers urge you to buy overpriced or worthless plans.
• **"Free" trial offers**. Some companies use free trials to sign you up for products then they bill you every month until you cancel.

Join the National "Do Not Call" List

Register your home and mobile phone numbers with the National Do Not Call Registry. This won't stop all unsolicited calls, but it will stop most. **www.donotcall.gov.**