CONTACT NUMBERS

Federal Trade Commission
1-877-438-4338
www.ftc.gov/idtheft

Internet Crimes Complaint Center
www.ic3.gov

Securities Exchange Commission
1-800-732-0330
www.sec.gov

Internal Revenue Service
1-800-829-1040
www.irs.gov

Florida Attorney General/Elder Abuses
1-850-414-2000
www.elderaffairs.state.fl.us

FBI
1-202-324-3000
www.fbi.gov

Better Business Bureau
1-561-842-1918
www.bbb.org

Do Not Call List
1-888-382-1222
www.donotcall.gov

CREDIT BUREAUS

Contact one only, they share reporting

Equifax 1-800-525-6285
www.equifax.com

Transunion 1-800-680-7289
www.transunion.com

Experian 1-888-397-3742
www.experian.com

VAST

Volunteers Against Scams Team

The mission of the Volunteer Against Scams Team (VAST) is to advocate and assist citizens of Palm Beach County who have been targeted as victims of financial crimes, VAST core objectives include preventing additional victimization and providing assistance in recovering from crimes involving identity theft, fraud and other mainstream financial crimes.

The primary goal of VAST is to educate citizens to prevent scam victimization, provide information with regard to available resources and to "harden the target" against future financial victimization and loses.

For more information call the
Community Services Office
561-688-3970

PBSO #0255 REV. 10/15

VAST

Volunteers Against Scams Team

Palm Beach County Sheriff's Office
561-688-3000
3228 Gun Club Road, West Palm Beach, FL 33406
www.pbso.org

TYPES OF SCAMS

All scams fall into one of eight categories

1. Identity Theft
Stealing your personal information and illegally using it.

2. Counterfeit Cashiers' Check
Giving you a counterfeit check in exchange for your personal check.

3. Phishing and Spoofing
Forged electronic documents e-mailed to obtain your personal information.

4. Investment Fraud
Fraudulent schemes and deceptions relating to various investments.

5. Ponzi Schemes
Pyramid investing returns from new investors used to pay existing investors.

6. Spam
Unsolicited emails sent to obtain information and can include bogus offerings.

7. Telemarketing Scams
Bogus offers via telephone, fax and text.

8. Credit Card Fraud
Illegally obtaining your credit card information and using it.

PREVENTION TIPS

DO


* Read your bank, credit card and account statements.
* Shred documents that show your personal information.
* Check credit report yearly.
* Be on the "Do Not Call" list.
* Use Spam filters.
* Use anti-virus and malware programs.
* Call the Better Business Bureau or SEC.
* Research the company.

DON'T


* Open emails if you don't know the source.
* Respond to emails, text and phones messages requesting personal information.
* Leave your purse unattended.
* Provide financial information over the phone to unfamiliar companies.
* Be pushed into a hasty decision.
* Use passwords of pets or commonly used names.

RED FLAGS
* "If it sounds too good to be true it is"
* "I guarantee it" or "You can trust me"
* "Let's seal it with a handshake"

SCAMMED? CONTACT

- **Local Police**
  File report
- **Financial Institution**
  Close accounts if compromised
- **Credit Bureaus**
  Place fraud alert on account and order credit report
- **Federal Trade Commission**
  File fraud affidavit
- **Better Business Bureau BBB**
  File complaint

FREQUENTLY ASKED QUESTIONS

1. ***What risks are there in using debit cards?***

   Debit cards are considered a risky form of payment. They provide access to your personal bank account. Even worse, they do not provide the same protections as credit cards.

2. ***Is there a risk in using credit cards in restaurants?***

   The risk of using a credit card in a restaurant is the card leaves your sight and your personal information could be illegally scanned. An option in this case is using a cash payment but some customers may find this method impractical.

4. ***Why do I continue to receive calls from telemarketers after I went on the no call list?***

   The Do-Not-Call registry does not cover all unwanted calls, such as calls from charities, non-commercial calls, etc. Pre-recorded telemarketing "robocalls' are illegal, but continue to be a major problem. You can file a complaint with the FTC by phone, fax or internet. Violators are subject to substantial penalties.

5. ***Can I eliminate my address from my checks?***

   Yes. You can also eliminate your phone number and social security. When you present a check to a merchant you will be asked to provide your driver's license or I.D. to verify you are the owner of the check.

6. ***How can I protect my computer?***

   Do not open emails from unknown sources. Use anti-virus and anti-spyware program, and a firewall on your computer. Also, set your computer's operating system, web browser, and security system to update automatically.

7. ***Why should I report an I.D. theft to the Federal Trade Commission?***

   You want to file a complaint with the FTC and receive an FTC Fraud Affidavit. The Affidavit together with your police report creates an Identity Theft Report. It will prove to third parties that you have been a victim of an identity theft.

8. ***If I shop or bank online, how can I protect myself?***

   Use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address: "s" is for secure. If you use a public wireless networks such as those at coffee shops, bookstores, etc., don't send information to any website that isn't fully encrypted.