BUSINESS, TECHNOLOGY & IDENTITY THEFT
In accordance with federal law and U.S. Department of Justice policy, this organization is prohibited from discriminating on the basis of race, color, national origin, religion, sex, age, or disability.

To file a complaint of discrimination call the Department of Legal Affairs, Federal Discrimination Complaint Coordinator, PL-01 The Capitol, Tallahassee, Florida, 32399, or call 850-414-3300, or write Office of Civil Rights, Office of Justice Programs, U.S. Department of Justice, 810 7th Street, NW, Washington, DC 20531 or call 202-307-0690 (Voice) or 202-3087-2027 (TDD/TYY).

Individuals who are hearing impaired or have speech disabilities may also contact OCR through the Federal Relay Service at 800-877-8339 (TTY), 877-877-8982 (Speech), or 800-845-6316 (Spanish).
In Florida the FTC reported 200,392 Fraud Complaints.
Identity theft happens when someone uses your personal identifiable information without your permission to commit fraud or other crimes.
Personal identification information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.
FTC Top Reported Identity Theft Crimes in Florida

1. Government & Document Fraud
2. Credit Card Fraud
3. Bank Fraud
4. Phone & Utilities Fraud
5. Employment Fraud
6. Loan Fraud
Tax refund fraud results from the filing of U.S. income tax returns using false information and someone’s personal information, without permission, with the intent to obtain tax refunds.
(a) “Breach of security” or “breach” means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

- Malicious Attacks 37%
- Negligence/Human Factor 35%
- System Glitches 29%
Small Businesses Have Major Exposure to Data Breaches

As small businesses begin to utilize new technologies, such as cloud computing, the risk of cyberattacks and data breaches is increasing.

For this reason, purchasing liability insurance that protects against these risks should be a priority for small businesses using these technologies, as a single lawsuit stemming from compromised business.

According to a recent survey conducted by the Ponemon Institute, more than experienced at least one data breach, and many have reported multiple incidents.

The primary causes of attacks included employee or contractor mistakes, lost storage media as well as procedural mistakes.

“Smaller companies are targeted by data thieves, but they often don’t know how they keep on customers and employees is lost or stolen,” said Eric Cennik, vice president, primary service. “Failing to act in a timely and effective way can harm the reputation of business stakeholders.”

FTC can sue companies hit with data breaches, court says

Agency secures major victory in legal battle with Wyndham Worldwide hotel operator

By Jaikumar Vijayan

Computerworld | Apr 10, 2014 2:23 PM PT

A federal court in New Jersey this week affirmed the Federal Trade Commission’s contention that it can sue companies on charges related to data breaches, a major victory for the agency.

Judge Esther Salas of the U.S. District Court for the District Court of New Jersey ruled that the FTC can hold companies responsible for failing to use reasonable security practices.
Follow the Numbers…

90% of data breaches impact small businesses

Average cost of a data breach for a small business: $360,000

31% of customers terminate their relationship with the small business
FIVE PRINCIPLES TO SAFE GUARD PERSONAL INFORMATION

1. Take Stock
2. Scale Down
3. Lock It
4. Destroy It
5. Plan Ahead
Know what personal information you have in your files

- File cabinets
- Computers
- Laptops
- Flash drives
- Disks
- Home computers
- Cell phones
- Contractors
- Websites
- Other equipment

Know who, why, what, how and where the information comes from
Use Social Security numbers only for required and lawful purposes

Look @ web screens and eliminate information you don’t need

Keep credit card information only if you have a need for it
PROTECT THE INFORMATION THAT YOU KEEP

- **Employee/Contract Security**
  - Check references
  - Do background checks

- **Electronic Security**
  - Use an intrusion detection system
  - Use password-activated screen savers
  - Monitor traffic for signs of hacking
  - Use encryption if you allow remote access
  - Regular e-mail is not a safe way to send sensitive data

- **Physical Security**
  - Limit access to "need to go"
  - Lock file cabinets and office doors

- **Employee Training**
  - Put files away
  - Log off their computers
  - Do not share their passwords
PROPERLY DISPOSE OF WHAT YOU NO LONGER NEED

- Separate sensitive data from regular trash
- Shred burn or pulverize paper records
- Use wipe utility programs on old computers
- Employees working from home must follow the same procedure
Plan Ahead

Create A Plan To Respond To Security Incidents

- Designate a response team
- Create list of people to notify in the event of an incident
- Investigate security incidents immediately
- Disconnect a compromised computer from the internet
- Take steps to close off existing threats
State of Florida Division of Corporations

- Review Consumer Alerts
- Small Business Reference Guide
- Helpful Numbers Section

E-mail: corphelp@dos.myflorida.com
Contact the United States Internal Revenue Service Identity Theft Specialized Protection Unit at:

800-908-4490
To File a Fraud Complaint

Contact the Florida Attorney General
No Scam Hotline at:

Outside Florida call: 1-850-414-3990
1-866-9-NOSCAM
1-866-966-7226

www.myfloridalegal.com/identitytheft
Step (4) Report the incident to law enforcement. Request a copy of the police report. Some creditors will request to see the report to remove the dispute.

Step (3) If your checks have been stolen, stop payment on your checks. Only accept new checks. Close your checking and savings accounts and open new accounts.

Step (2) Gather the correct information. Make changes to existing accounts or contact your prior creditors to open new accounts. Creditors should be notified of the theft. A VOLUME: 1-888-333-0000

Step (1) Report the incident to the fraud department of the three major credit bureaus. Ask the fraud department of the three major credit bureaus to place a fraud alert on your credit reports. Identity Theft is a crime. Identify thieves who steal your personal and financial information, and do not click on links in the messages that ask for personal or financial information. Do not reply to an email or pop-up.

What Is Identity Theft?

If You Are A Victim

Reduce Your Risk
KEY: KEEP YOUR IDENTITY SAFE

.Identity Theft

RESOURCES & INFORMATION

The Office of the Attorney General is an equal opportunity provider and employer.

ID theft - Department of Justice

https://www.usdoj.gov/identitytheft/index.html

Motor Vehicle Fraud Section 1-850-414-3909, 1-888-397-2972

File your driver license if you are a victim of identity theft or fraud.

U.S. Department of State 1-877-487-2778

Report lost or stolen passport

To check or clear criminal history for

https://www.uscis.gov/egov/af clinicians.aspx

Compromised Identity 1-850-410-7898

Fraudulent data - Florida Department of Law Enforcement (FDLE)

https://www.fdle.state.fl.us/ConductHome.aspx

Translation


Check Verification Companies

1-800-680-7289


http://www.equifax.com/1-800-525-6285

http://www.transunion.com

Place Fraud Alerts

https://www.idtheft.gov

Remove your personal identifiers from

http://www.idtheft.gov/ue_Finality_Projection

Serve Identity Protection Specialized Unit

https://www.irs.gov/identitytheft

Report ID theft and fraud to the Federal

https://www.identitytheft.gov

In Florida

General's Office 1-850-414-3909, 1-888-397-2972

General's Office 1-866-9-NOSCAM or

To file a complaint for fraud with the Attorney General.

RESOURCES & INFORMATION

Identity Theft