

Attention Holiday Shoppers: Tips For Victims Of Identity Theft

By Scott Callahan

We've all heard about the massive data breaches that have led to the thefts of personal information of millions of consumers from large businesses. These days, thieves are targeting consumers in countless ways – skimming devices attached to ATM machines, dumpster diving, shoulder surfing at cash registers, and old-fashioned purse-snatching. It's infuriating.



Identity theft can expose banking information, Social Security numbers, usernames, passwords, and even family medical histories. The financial impact can be devastating. So can the emotional toll.

Credit card theft is the most common form of identity theft. But, other areas are also increasingly popular:

- Medical Identity Theft. Victims getting billed for medical services or prescriptions they never received. Or, victims being denied health insurance or health benefits because someone else's health information actually shows up in their medical records.
- Utility Identity Theft. Thieves using your information to set up utility accounts for their use.
- Tax Identity Theft. Filing false tax returns and collecting a refund under a victim's name.

So, what should you do in the face of identity theft?

Prevent fraud in the first place.

- Make a list of all of your credit card, banking, and service provider accounts, and keep the list in a safe place.
- Change your passwords frequently; use at least 10-digit passwords consisting of letters and numbers; the longer the better (avoid birthdays and your kids' names).
- Keep your account and password information secure/encrypted.
- Order a copy of your credit report from the credit bureaus and confirm the accounts belong to you and that the account balances are accurate.

But what if it's too late and the worst happens?

First, take a deep breath. Then, do what you can to stop the fraud immediately:

- Immediately notify all account providers (credit cards, bank, phone, utilities).
- Contact the three national credit reporting agencies (Equifax, Experian, TransUnion). Request a "fraud alert" on your credit account. This will last for 90 days and can be renewed. Also, request a "security

freeze.” This will stop any new accounts from being fraudulently opened.

- If your Social Security number is stolen, notify the Social Security Administration and the Internal Revenue Service. Watch your annual Social Security income report for errors.
- Request a free copy of your credit report from one of the three agencies mentioned above. If errors are found, dispute them in writing with both the credit reporting company as well as the fraud department for the business that reported the error to the credit agency. Also, request that the credit agency and business “block” the error from appearing on your credit report since you are the victim of identity theft.

Next, create an “Identity Theft Report.” This is a combination of an Identity Theft Affidavit and a police report:

- Submit a report about the theft to the FTC (Federal Trade Commission). An online form can be found and submitted on the FTC website at www.ftc.gov. Be sure to print a copy for your records. It will serve as your Identity Theft Affidavit.
- File a police report and provide law enforcement with your FTC Identity Theft Affidavit. Be sure to get a copy of the police report. Together, these two documents will serve as your Identity Theft Report which will help you deal with debt collectors, credit reporting agencies, and businesses inquiring about your credit.

The next step is to monitor, monitor, and monitor. Be diligent about keeping track of your phone calls, emails and letters sent to resolve the problem. Put as much as you can in writing. Log calls, names, dates, and times.

Finally, if the thief is caught, contact the district attorney’s office and be aggressive about having criminal charges brought and providing testimony. On the civil side, a lawsuit against the thief is possible, but the likelihood of recovery may be very slim.

While identity theft is not limited to the holidays, ‘tis the season for people who are looking for ways to be you.



Law Office of Scott P. Callahan, P.C.

23501 Cinco Ranch Blvd.
Suite B240
Katy, TX 77494
Telephone: 713-888-9000
Email: Scott@scottcallahan.com
Website: www.scottcallahan.com

The information in this column is not intended as legal advice, but to provide a general understanding of the law. Readers with legal issues, including those whose questions are addressed here, should consult attorneys for advice on their particular circumstances.

Scott Callahan is a personal injury trial lawyer with offices in Katy and Houston. He has been practicing law for more than 20 years and is Board Certified in Personal Injury Trial Law by the Texas

Board of Legal Specialization. His email is scott@scottcallahan.com and the law firm's website is www.scottcallahan.com.