

NEW JERSEY DIVISION OF CONSUMER AFFAIRS

FIGHTING



FRAUD

If You Become a Victim of Identity Theft

Identity theft – the misuse of one’s personal and financial information by a criminal who steals money from the victim’s accounts or takes out loans in the victim’s name, leaving the victim in debt – can cause very real heartache and aggravation for its victims.

But there is good news. The U.S. Justice Department, Bureau of Justice Statistics, found that victims of identity theft can resolve the financial and credit problems that result from this crime. The majority of victims were even able to resolve these issues in less than one day, once they became aware of the crime and took concrete action.

WHAT CAN YOU DO?

All New Jerseyans who believe they were exposed to identity theft – whether through a data breach, a phishing scam, or the theft of their passport or other documents – can take the following steps for self-protection.

- File a complaint with the Federal Trade Commission at www.ftc.gov/complaint or 877-438-4338. Your completed complaint is called an "FTC Affidavit." You will want to bring a copy of the FTC Affidavit to your local police department; see Step 2.
- File a report with your local police department, and bring the police a copy of your FTC Affidavit. Once your police report has been filed, request a copy so it will be available to send to credit reporting agencies and creditors.

- Obtain a copy of your credit report from all three credit reporting agencies. Contact them at:

Equifax Credit Information Services
Consumer Fraud Division

(800) 525-6285 • www.equifax.com

Experian

(888) 397-3742

www.experian.com/consumer

Trans Union

Fraud Victim Assistance Department

(800) 680-7289 • www.tuc.com

Tell these credit reporting agencies that you suspect you were exposed to identity theft, and ask that all of your accounts be flagged with a fraud alert. This will alert any creditors, in case an identity thief attempts to obtain a credit card or loan in your name.

- Keep a close watch on the activity on your credit or debit cards. Many card issuers offer online account access. If you can, check the accounts daily. If you are unable to access this information online, call the numbers on the back of the affected cards.

Continued on back

Be an Informed Consumer ... We can Help!

800-242-5846 ■ NJConsumerAffairs.gov

- Contact all credit card companies, creditors, banks, and any financial institutions with which you do business. Close the affected credit card and bank accounts, and get replacement cards with new account numbers. Change any passwords on the accounts, including PINs. Follow up all telephone contact with a written confirmation.
- Contact the United States Social Security Administration at:

Social Security Administration
Social Security Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235

(800) 269-0271

TTX: (866) 501-2101

www.ssa.gov/oig/hotline

- Keep a complete set of records. Keep a log with notes on all telephone conversations with credit reporting bureaus, creditors, or debt collection agencies. Confirm all telephone conversations in writing. Keep copies of all paper or electronic correspondence you send and receive related to the suspected identity theft. Send correspondence by certified mail, return receipt requested. Keep a record of the time spent and any expenses you incurred, in case it one day becomes possible to claim restitution in a judgment against the identity thief.

- You can also contact nongovernmental nonprofit groups established to provide assistance to victims of identity theft. For example:

Identity Theft Resource Center

(888) 400-5530

www.idtheftcenter.org

AN ADDITIONAL WORD ABOUT DATA BREACHES

Several companies affected by recent data breaches have offered free credit monitoring services to affected consumers. Consumers should consider taking advantage of these offers – but should first take the time to verify that any communication about such an offer is genuine.

Scammers have been known to contact consumers by email or phone, while pretending to offer information and help about a data breach. Their motivation is to fool unsuspecting consumers into downloading computer viruses, sending money, or giving away their personal information.

The best self-protection is to verify any suspicious email with the purported sender, through a separate medium such as a phone call. If there is any doubt about a message, simply delete it.



Be an Informed Consumer ... We can Help!

800-242-5846 - NJConsumerAffairs.gov