

## **Credit Card Fraud:**

Credit card fraud is a form of identity theft that involves an unauthorized taking of another's credit card information for the purpose of charging purchases to the account or removing funds from it. Federal law limits cardholders' liability to \$50 in the event of credit card theft, but most banks will waive this amount if the cardholder signs an affidavit explaining the theft.

Credit card fraud schemes generally fall into one of two categories of fraud: application fraud and account takeover.

Application fraud refers to the unauthorized opening of credit card accounts in another person's name. This may occur if a perpetrator can obtain enough personal information about the victim to completely fill out the credit card application, or is able to create convincing counterfeit documents. Application fraud schemes are serious because a victim may learn about the fraud too late, if ever.

Account takeovers typically involve the criminal hijacking of an existing credit card account, a practice by which a perpetrator obtains enough personal information about a victim to change the account's billing address. The perpetrator then subsequently reports the card lost or stolen in order to obtain a new card and make fraudulent purchases with it.

Another common method used to achieve an account takeover is called "skimming." Skimming schemes occur when businesses' employees illicitly access to customers' credit card information. These employees then either sell the information to identity thieves or hijack the victim's identities themselves.

Technological advances have also created avenues for credit card fraud. With online purchasing now common, perpetrators need no physical card to make an unauthorized purchase. Additionally, electronic databases containing credit card data may be hacked or crash on their own, releasing customers' credit card information, putting the security of many accounts at risk at once. (Provided by Legal Information Institute, Cornell University Law School.)

## **What you need to do:**

REVIEW your credit report every year to make sure there haven't been any new credit cards or other accounts issued (to someone other than you) and to make sure there haven't been inquiries by people you haven't initiated business with. There are also services you can subscribe to (such as Credit Expert) that will alert you to any changes in your credit file.

REVIEW your monthly credit card statement each month to make sure there aren't any charges showing up that aren't yours. Also, make sure you get a monthly statement. If the statement is late, contact the credit card company. You never know when someone may have turned in a change-of-address form so they could make a few more weeks of purchases on your credit card without you noticing.

If you're ever denied credit, **FIND OUT WHY**, especially if you haven't reviewed your credit report lately. This may be the first indication you get that someone has stolen your identity and is racking up charges in your name.

REACT QUICKLY if a creditor or merchant calls you about charges you didn't make. This too may be the first notice you get that someone has stolen your identity. Get as much information from them as you can and investigate immediately.

GUARD deposit slips as closely as you do checks. Not only do they have your name, address and account number printed on them, but they can also be used to withdraw money from your account. All a thief has to do is write a bad check, deposit it into your account and use the "less cash received" line to withdraw your money.

### **If It Happens To You**

Contact the Credit Bureaus listed below.

#### **Equifax**

Credit Information Services - Consumer Fraud Div.

P.O. Box 105496

Atlanta, Georgia 30348-5496

Tel: (800) 997-2493

[www.equifax.com](http://www.equifax.com)

#### **Experian**

P.O. Box 2104

Allen, Texas 75013-2104

Tel: (888) EXPERIAN (397-3742)

[www.experian.com](http://www.experian.com)

#### **TransUnion**

Fraud Victim Assistance Dept.

P.O. Box 390

Springfield, PA 19064-0390

Tel: (800) 680-7289

[www.transunion.com](http://www.transunion.com)

What if you find out through a phone call from a creditor, a review of your credit report, or even a visit from the police, that your identity has been stolen? The first thing to do is report the crime to the police and get a copy of your police report or case number. Most credit card companies, banks, and others may ask you for it in order to make sure a crime has actually occurred.

You should then immediately contact your credit card issuers, close your existing accounts and get replacement cards with new account numbers. Make sure you request that the old account reflect that it was "closed at consumer's request" for credit report purposes. It is also smart to

follow up your telephone conversation with letters to the credit card companies that summarize your request in writing.

Close any accounts the thief has opened in your name. If you open new accounts yourself, make sure you request that passwords be put on those accounts. As with any password, make sure you use something that is not obvious to others. Don't use your mother's maiden name, the last four digits of your social security number, or anything else that would be obvious.

Next, call the fraud units of the three credit reporting bureaus and report the theft of your credit cards and/or numbers. Ask that your accounts be flagged with a "fraud alert." This usually means that someone can't set up a new account in your name without the creditor calling you at a phone number you specify. Verify with the credit bureau representative you speak with that this will happen, and provide them with the number at which you want to be reached. The downside of this is that you won't be able to get "instant credit" at department stores. This flag, also known as a "victim's statement," is the best way to prevent unauthorized accounts.

Make sure to keep a log of all conversations with authorities and financial entities, and keep copies of any documentation you provide to them.

If your social security number has been used, notify the Social Security Administration's Office of Inspector General.

File a complaint with the Federal Trade Commission (FTC) by contacting the FTC's Consumer Response Center. The FTC is the federal clearinghouse for complaints by victims of identity theft. The FTC does not have the authority to bring criminal cases, but it does assist victims by providing information to help them resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for further action.

The FTC also has an online identity theft complaint form that can help them gather information about identity theft and lead to law enforcement actions.

If you have any question please contact us at the Lincoln County Sheriff's Office, (509) 725-3501.