Protecting Your Credit from ID Fraud

BACKGROUND

Credit-related identity fraud represents less than one third of identity fraud cases, but is the type of identity fraud that many consumers fear most. No one wants to face ruined credit and aggressive collection agencies. There are many types of credit-related identity fraud, but the cases can be put into two broad categories: existing account fraud and new account fraud.

EXISTING ACCOUNT FRAUD

Under Existing Account Fraud, someone gets hold of a valid credit account and misuses that account. If you are the victim, the account that has been misused is one that you established and are aware of.

You may have lost your purse or wallet, in which case the person committing the fraud could be using the actual credit card associated with the account. More often, the account number has been copied from another transaction or hacked out of a computer. Your account number is then either embossed onto a phony credit card or, more simply, used to make purchases online or by telephone.

In some cases, the thief will change the account profile information. This is sometimes referred to as "account takeover." One typical ploy is to change the address where statements are sent. If the credit card bill doesn't come to you, it may take weeks or months before you realize that your account is being misused.

NEW ACCOUNT FRAUD

Under New Account Fraud, someone gets hold of your personal identifying information and uses that information to apply for a new credit account. If you are the victim, the account is one that you did not establish and – at least for some period of time – are not aware of.

Some thieves establish new credit accounts using the victim's true address. Such accounts are generally drained quickly because the thief knows that the activity will become visible to the victim when the first statement is mailed out.

Other thieves establish new credit accounts using a fictitious address or the thief's address. Because the victim is not receiving bills, the fraudulent accounts can continue for many months before the victim becomes aware of a problem. The perpetrator of the fraud may even make some payments on the account to keep it going and possibly attain a higher credit limit.

MERCHANTS INSURANCE GROUP

One simple version of this fraud uses the credit offers that many consumers receive in the mail. Such offers are often coded in such a way that they are tied to the credit of the person the offer is addressed to. If you throw away the offer letter without shredding it, an identity thief who finds that letter in the trash can use it to establish a new account using your credit – and then change the mailing address.

LOSS DETECTION AND RESPONSE

There are two key steps to detecting Existing Account Fraud:

- Review your monthly statement on every credit account in detail. Watch for any charges for goods or services that you did not receive.
- Make sure that you receive a statement each month on all of your accounts. Failure to receive a statement could indicate that someone has changed your address.

The best way to detect New Account Fraud is to check your credit file as maintained by one or more of the national credit repositories, also known as the credit bureaus. The three bureaus are Equifax, Experian and TransUnion. Under federal law, consumers are eligible to receive one free credit report from each bureau once every 12 months. The best way to do this is through the website at www.AnnualCreditReport.com or by phone at 1-877-322-8228.

If you have any reason to believe your identity is being misused, please contact the ID Recovery Help Line at 1-800-414-9792.

MERCHANTS INSURANCE GROUP

Merchants Insurance Group includes Merchants Mutual Insurance Company and Merchants Preferred Insurance Company.