

DCC DOLLARS & \$ENSE

Volume II, Issue I

February 1, 2004

Identity Theft

Explained by the Federal Trade Commission (FTC)

Special points of interest:

- Client Question and Answers.
- Identity Theft

Fact & Fallacy

Fallacy: I will be liable for all of the transactions that take place in the event of Identity Theft.

Fact: The maximum liability in the event of identity theft is \$50.00. Once a consumer is aware that there has been theft of their identity they need to file a fraud report and this will limit the number of new transactions. In turn, that will limit the amount of a consumer's liability.

Identity theft became a very common thing in the early nineties. Since then the FTC has exercised a vast amount of resources to help to prevent it. Included in those have been several publications to help to educate consumers. The following are excerpts from the FTC's educational material.

Skilled identity thieves use a variety of methods to gain access to your personal information. For example:

- 1) They get information from businesses or other institutions by:
 - Stealing records from their employer,
 - Bribing an employee who has access to these records, or
 - Hacking into the organization's computers.
- 2) They rummage through your trash, or the trash of businesses or dumps in a practice known as "dumpster diving."
- 3) They obtain credit reports by abusing their employer's authorized access to credit reports or by posing as a landlord,

employer, or someone else who may have a legal right to the information.

4) They steal credit and debit card numbers as your card is processed by using a special information storage device in a practice known as "skimming."

5) They steal wallets and purses containing identification and credit and bank cards.

6) They steal mail, including bank and credit card statements, pre-approved credit offers, new checks, or tax information.

7) They complete a "change of address form" to divert your mail to another location.

8) They steal personal information from your home.

9) They scam information from you by posing as a legitimate businessperson or government official.

Once identity thieves have your personal information, they may:

- 1) Go on spending sprees purchasing big-ticket items like computers that they can easily sell.

NEW! Customers ask DCC for the answers to their financial questions.

We try to provide a variety of information to consumers and to be here to answer any questions that they may have. Now, we have set up to have a way for clients to email or write in questions that they would like answers to or topics they would like to see dis-

cussed. If you have a question or topic, email it to questions@delraycc.com and you could see your questions answered online and in our newsletter. Helping not only yourself, but other clients who may have had the same question or concern.

Identity Theft Cont.

2) Open a new credit card account, using your name, date of birth, and SSN. When they don't pay the bills, the delinquent account is reported on your credit report.

3) Change the mailing address on your credit card account. The imposter then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before you realize there's a problem.

4) Take out auto loans in your name.

5) Establish phone or wireless service in your name.

6) Counterfeit checks or debit cards, and drain your bank account.

7) Open bank accounts in your name and write bad checks on that account.

Customers Ask DCC

Question I've been offered a settlement from one of my creditors for 60% of the balance that I currently owe. That is pretty much the total of what I had actually charged, the rest were just fees. I haven't been able to pay them in several months and they've charged off my account. Is it worth it to do a settlement, or will that be worse than the charge off?

John G, Dallas Texas

Answer: John, it's a good question. You need to look at the amount that you would be saving and your ability to meet their payment schedule. In most cases a lender will require either payment in full, or three equal installments to meet the settlement amount. Unfortunately, in order for the amount saved to be worthwhile, the payment schedule is usually pretty steep.

With the account being charged off, that will be the predominant factor on your credit score. [in regards to this account] A narrative code of "settlement accepted" would not have much more of an impact. It does however show future lenders that previous creditors were not paid in full.

Steps You Can Take

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from any of three major credit bureaus. If you find inaccurate information, check your reports from the other two credit bureaus. Of course, some inaccuracies on your credit reports may be because of computer, clerical, or other errors and may not be a result of identity theft. Note: If your personal information has been lost or stolen, you may want to check all of your reports more frequently for the first year. Federal law allows credit bureaus to charge you up to \$9 for a copy of your credit report. Some states may allow a free report or reduced rates.

How Can You Tell If You're A Victim of Identity Theft?

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

1) Failing to receive bills or other mail signaling an address change by the identity thief.

2) Receiving credit cards for which you did not apply;

3) Denial of credit for no apparent reason; or

4) Receiving calls from debt collectors or companies about merchandise or services you didn't buy.

Place a fraud alert on your credit reports and review your credit reports.

Call the toll-free fraud number of anyone of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

- **Equifax** — To report fraud, call: 1-800-525-6285,
- **Experian** — To report fraud, call: 1-888-EXPERIAN
- **TransUnion** — To report fraud, call: 1-800-680-7289

Once you receive your reports, review them carefully. Look for inquiries you didn't initiate, accounts you didn't open, and unexplained debts on your true accounts. You also should check that information such as your SSN, addresses, name or initial, and employers are correct. Inaccuracies in this information also may be due to typographical errors. Nevertheless, whether the inaccuracies are due to fraud or error, you should notify the credit bureau as soon as possible by telephone and in writing. You should continue to check your reports periodically, especially in the first year after you've discovered the theft, to make sure no new fraudulent activity has occurred. The automated "one-call" fraud alert process only works for the initial placement of your fraud alert. Orders for additional credit reports or renewals of your fraud alerts must be made separately at each of the three major credit bureaus.