CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™
ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2016 Atlanta Conference
May 19-20, 2016 in Atlanta, GA

Identity Theft and Identity Fraud - Does it Affect Insurance Claims?

I. The Scope of the Problem

Definition of Identity Theft

Identity theft is the act of taking someone's personal information, such as their name, birth date, social security number, etc., and using it to impersonate a victim, steal from bank accounts, establish phony insurance policies, open unauthorized credit cards or obtain unauthorized bank loans. In some more elaborate schemes, criminals use the stolen personal information to get a job, rent a home or take out a mortgage in the victim's name.

In the United States, identity theft became a federal crime on October 30, 1998 through the enactment of the Identity Theft and Assumption Deterrence Act of 1998, (a) (7). According to the Act, identity theft occurs when a person:

"Knowingly transfers, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

Definition of Identity Fraud

Identity fraud occurs when individuals knowingly and without lawful authority produce an identification document, authentication feature, or a false identification document with the intent to defraud others.

The identification document is reproduced using, without authority, personal identifying information from another person. The defrauded victims in this case are the person whose personal identifiers were used and the organization(s) that either compensate the identity theft victim or take the loss for assets purchased or obtained by the identity criminal, as in the case of a fraudulent insurance claim.

The identification document can also be made up of random names and numbers to create a new identity. This is called synthetic identity theft. The victim in this case is the organization(s) that looses profits from assets purchased by the identity criminal.

Identity Theft and Identity Fraud Affect Us All

17.6 million Americans, or 7% of US residents aged 16 or older, were victims of identity theft in 2014. 86% of these victims experienced the misuse of an existing credit card or bank account. 4% of these victims had their personal information stolen and used to open a new account or for other fraudulent activity. Many victims experienced multiple types of identity theft during the most recent incident.

Most identity theft victims (45%) uncovered the scheme when their financial institution contacted them about suspicious activity. A significantly smaller amount of victims uncovered the problem when they noticed fraudulent charges on their account (18%). Most identity theft victims did not know how the offender obtained their information, and almost all (9 in 10) did not know anything about the offender.

SOURCE: US Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014, Erika Harrell, Ph.D.*

Victim Demographics

More women (9.2 million) were victims of identity theft than men (8.3 million). Whites experienced identity theft at higher rates than African Americans or Hispanics or "other races". Victims ages 25 to 34 had the highest rate of identity theft, compared to all other age groups. Persons in households with an annual income of $75,000 or more had the highest prevalence of identity theft, compared to those in all other income brackets.

SOURCE: US Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2014, Erika Harrell, Ph.D.*

`

II. Preventative Measures

Avoiding Theft

- Keep the amount of personal information in your purse or wallet to the bare minimum.
- Avoid carrying additional credit cards, your social security card or passport unless absolutely necessary.

- Guard your credit card when making purchases.

- Shield your hand when using ATM machines or making long distance phone calls with phone cards. Don't fall prey to "shoulder surfers" who may be nearby.

- Always take credit card or ATM receipts. Don't throw them into public trash containers, leave them on the counter or put them in your shopping bag where they can easily fall out or get stolen.

- Do not give out personal information. Whether on the phone, through the mail or over the Internet, don't give out any personal information unless you have initiated the contact or are sure you know who you are dealing with and that they have a secure line.

- Proceed with caution when shopping online. Use only authenticated websites to conduct business online. Before submitting personal or financial information through a website, check for the locked padlock image on your browser's status bar or look for "https://" (rather than http://) in your browser window. If you have any concerns about the authenticity of a Web page, contact the owner of the site to confirm the URL.

- Be aware of phishing and pharming scams. In these scams, criminals use fake emails and websites to impersonate legitimate organizations. Exercise caution when opening emails and instant messages from unknown sources and never give out personal, financial or password related information via email.

- Make sure you have firewall, anti-spyware and anti-virus programs installed on your computer. These programs should always be up to date.

- Monitor your accounts. Don't rely on your credit card company or bank to alert you of suspicious activity. Carefully monitor your bank and credit card statements to make sure all transactions are accurate. If you suspect a problem, contact your credit card company or bank immediately.

- Order a copy of your credit report from each of the three major credit bureaus. A new law that took effect December 1, 2004, entitles you to one free credit report per year. Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Make sure it's accurate and includes only those activities you've authorized.

- Place passwords on your credit card, bank and phone accounts.

- Avoid using easily available information like your mother's maiden name, your birth date, any part of your Social Security number or phone number, or any series of consecutive numbers. If you suspect a problem with your credit card, change your password.

- Shred any documents containing personal information such as credit card numbers, bank statements, charge receipts or credit card applications, before disposing of them.

SOURCE: Insurance Information Institute:
http://www.iii.org/article/identity-theft-insurance

Available Coverage

The National Association of Insurance Commissioners ("NAIC") estimates the cost of identity theft insurance coverage to range from $25 to $60 per year. This type of insurance includes credit alerts, account and credit monitoring, and reimbursement for the costs associated with repairing your credit history if you become a victim. The policies do not cover monetary losses.

According to the NAIC, most policies typically have limits ranging from $10,000 to $15,000. Deductibles require an insured to pay the first $100 to $500 of costs required to restore his or her financial reputation.

Many homeowner carriers are offering this type of "identity theft restoration" coverage through endorsements.

See, http://money.usnews.com/money/blogs/my-money/2014/03/24/should-you-buy-identity-theft-insurance

For More Information Go To:

Federal Trade Commission, Consumer Information
http://www.consumer.ftc.gov/features/feature-0014-identity-theft