ALERT
AUGUST 24, 2010

GLOBAL INSURANCE GROUP
News Concerning
Recent Professional Liability Issues

COZEN O'CONNOR
www.cozen.com

IDENTITY THEFT: OUR CHILDREN AT RISK

Richard J. Bortnick • 610.832.8357 • *rbortnick@cozen.com*
Amanda M. Lorenz • 619.234.1700 • *alorenz@cozen.com*

Interviewing for your first job as a teenager is as exciting as it is intimidating. Thoughts of what to do with your first paycheck consume your mind as you rehearse your best do-you-want-fries-with-that smile. The interview proceeds flawlessly, and you start to count the dollar signs as you await the job offer. But, imagine your surprise when you are informed that you did not get the job because your background check revealed that you are more than $75,000 in debt and five years behind in child support payments for your 11-year-old child—a terrifying thought considering you are only 16 years old.

Adults are not the only victims of identity theft. Child identity theft is an increasing and understated crime. A child's Social Security number ("SSN") is the perfect target, as the theft typically goes undetected until years after the crime has taken place. Indeed, the crime might not be discovered until the rightful owner/victim uses his or her SSN for the first time years later. This revelation often occurs when the victim applies for his or her first job or financial aid before college.

The scheme works as follows: businesses are using various techniques to search the Internet for dormant SSNs. These numbers often belong to long-term inmates, dead people, or children. Obtaining them is not as difficult as one may think. SSNs are formulated systematically depending on age, geographic location, and when the number is issued. Once it has been determined that no one is actively using the number to obtain credit, the numbers are offered for sale.

For example, dormant numbers are being sold to fraudsters who want to establish phony credit. Although some of the purchasers may be seeking a new number in hopes of rebuilding their financial position, most buyers use the numbers to run up large amounts of debt that they never intend to repay. Once the number is no longer useful (i.e. the credit is destroyed), a new number is purchased and the cycle continues.

Of course, selling SSNs is illegal. However, these businesses are not selling SSNs. Rather, they are selling a "CPN," which stands for "credit profile number," "credit protection number," or "credit privacy number." Complex disclaimers warning against using CPNs in place of SSNs make it difficult to prove that the businesses are actually selling SSNs. Such activities are even more difficult to prosecute. In addition, since these crimes often remain undetected for years, the businesses selling these numbers often no longer exist by the time the crime is discovered.

In an effort to protect minors' identities and credit issuers' portfolios, the Identify Theft Resource Center proposed the creation of a Minors 17-10 Database. The database would maintain a registry of all SSNs issued to minors younger than 17 years and 10 months and would provide credit issuers with a method to verify whether the CPN belonged to a minor. Regrettably, the proposed database has not yet been adopted or implemented.

A host of credit reporting agencies provide tools to protect against this type of fraud. However, they can be prohibitively expensive, particularly for small business owners. Until a system similar to the Minors 17-10 Database is put into place, businesses are encouraged to confirm and cross-reference as much of an applicant's information as possible.

One way to protect yourself or your child from identity theft is to routinely check your child's credit report for any activity. Also, if your child is receiving pre-approved credit card applications in the mail or telephone calls from telemarketers, such contacts provide indicia that your child's identity might be at risk. The earlier this crime is detected, the easier it is to remedy.

As for professional liability underwriters who insure or are looking to write small businesses and other credit providers, it is important to know that your policyholders are using all resources available to protect themselves and avoid losses, whether they be cyber-related or through brick and mortar operations. As President Obama recently observed, the private and public sectors need to work cooperatively to protect the nation's financial and cyber infrastructures. A key player in this effort is the insurance industry. Insurers need to be at the forefront and proactive. The risks simply are too great for them not to be.

Cozen O'Connor is a global leader in representing the insurance industry in coverage matters. For further analysis of CGL, D&O, E&O and other cyber law issues, please contact Richard Bortnick in our West Conshohocken office (rbortnick@cozen.com, 610-832-8357) or Amanda Lorenz in our San Diego office (alorenz@cozen.com, 619-234-1700).