Report Offers First Large-Scale Look at Child ID Theft

A new report issued by Carnegie Mellon CyLab Distinguished Fellow Richard Power offers startling details into how identity thieves target children for unused Social Security numbers. Based on identity protection scans of more than 40,000 children, CyLab found that 10.2 percent of them – 4,311 children – had someone else using their Social Security numbers. The youngest victim was just five months old, and the largest fraud totaled $725,000. "A child's identity is a blank slate, and the probability of discovery is low, as the child will not be using (a Social Security number) for a long period of time," the report said. "Parents typically don't monitor their children's identities."

In 2010, the Federal Trade Commission (FTC) received 250,854 complaints of identity theft. That figure includes the nearly 30,000 complaints received by the Internet Crime Complaint Center (IC3®), a partnership between the FBI, National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance. Of the 121,710 referrals IC3 made to law enforcement in 2010, identity theft ranked second (16.6 percent of all referrals). About 8 percent of the identity theft complaints tallied by the FTC involved victims age 19 and younger. Experts note that the number of complaints represents only a fraction of the actual number of identity thefts that occur every year. The FTC estimates that as many as 9 million people fall victim to identity theft annually. Nearly 1 in 4 U.S. households experienced at least one form of white collar crime (including identity theft) in 2010, according to NW3C's 2010 National Public Survey on White Collar Crime. However, only 11.7 percent of those victimizations were reported to law enforcement.

In the CyLab report, researchers point to illegal immigration, organized crime and personal relationships as the main forces driving child identity theft. About 70 percent of the compromised Social Security numbers were used to obtain loans or open credit accounts. The report offers some tips for parents trying to protect their children from fraud, including: Watch for mail in your child's name, such as pre-approved credit card offers. These could indicate a child has an open credit file. Children who use social networking sites are vulnerable to identity theft. Talk to them about safe online behavior. Parents should not use children's names to open credit accounts. This is called "friendly" identity theft, and it is a crime. To download a copy of the CyLab child identity theft report, go to www.cylab.cmu.edu.