01/02/2014

By John Breyault, Vice President of Public Policy, Telecommunications and Fraud, National Consumers League

For thirteen years, the crime of identity theft has generated more complaints to the Federal Trade Commission than another other fraud. In 2012, more than 12 million Americans were affected by identity theft , costing the U.S. economy $20.9 billion. Every three seconds, a consumer's identity is comprised by this pernicious crime.

Seven years ago, President George W. Bush, recognizing the seriousness of the threat of ID theft, created the federal Identity Theft Task Force . Made up of eighteen federal agencies, the task force was charged with implementing a range of recommendations to address the threat of ID theft. The task force made thirty-one recommendations, from reducing the use of Social Security Numbers by federal agencies, to improving coordination by law enforcement, to passing a national data breach notification standard, to name a few. The implementation of these recommendations by the federal government, as well as improved anti-fraud procedures in the private sector, has done much to make life harder on ID thieves.

Despite these advances, ID theft is still a major threat to consumers, business and the government. According to one conservative estimate , more than 1.1 billion records have been comprised by identity theft. Data breaches, which put information on millions of consumers in the hands of fraudsters, are still occurring at a rate of at least one per day.

Just as troubling, it appears that we may be on the cusp of a new wave of ID theft. With ever larger amounts of data being collected about consumers by government and the private sector, data breaches become more likely. Identity thieves are shifting towards scams that are harder to detect, such as tax-related ID theft and medical ID theft. And the criminal themselves — often located overseas — are becoming more professional and organized.

How will these new factors affect consumers' vulnerability to identity theft? What can we learn

from the last seven years of fighting this problem? What should consumers expect from regulators, law enforcement and the private sector as this crime evolves? In our recent whitepaper, *The State of Identity Theft in 2013*, we recommend a range of reforms to address the evolving identity theft threat, including updating the President's Identity Theft Task Force Report, enacting comprehensive data breach notification legislation, working more closely with foreign countries from which ID thieves may be operating, and providing stronger incentives for companies to better secure consumers' personal data.

Let's make 2014 the year we redouble our efforts to fight identity theft.