The Identity Theft Crisis: Will Tougher Penalties Alone Solve the Problem?

Harry A. Valetk
Special to law.com
08-05-2004

On July 15th, President Bush signed a tough new identity theft bill into law designed to increase the penalties for identity theft.

The new law, known as the Identity Theft Penalty Enhancement Act (Public Law No. 108-275) was introduced in the House by Representative John Carter, R-Texas, to create a new crime of "aggravated identity theft," and add two years to prison sentences for criminals convicted of knowingly transferring, possessing, or using a means of identification belonging to another person without lawful authority.

According to the bill's congressional findings, tougher penalties were needed because under current law many identity predators received little or no prison time. The House report specifically cited eight cases in which identity predators received relatively minor sentences for serious identity theft schemes. As such, leniency in sentencing was found to be a tacit encouragement to those arrested to continue to pursue this type of non-violent crime.

This will now change.

Under this new law, a prison term becomes mandatory. Individuals convicted of aggravated identity theft must receive a mandatory penalty enhancement of two years. Those who use personal data of another to commit "terrorist offenses" face an extra five years.

Federal judges will no longer be permitted to place identity thieves on probation, and sentencing cannot run concurrent with any other prison term, unless it is for another conviction under the same statute.

A NATIONAL CRISIS

Not surprisingly, this new statute comes at a time when identity theft is a national crisis. Indeed, identity theft remains by far the fastest growing white collar crime in the United States. And, despite various efforts by federal legislators to deter and punish identity predators with increasingly tougher penalties, the nation's identity theft crisis continues to deteriorate at a phenomenal pace.

According to a 2003 study by the Federal Trade Commission, approximately 10 million consumers fell victim to some form of identity theft within a 12-month period. The FTC also reported that losses to businesses and financial institutions totaled nearly $48 billion -- up from nearly $100 million in 2001 -- and consumers suffered about $5 billion in out-of-pocket expenses. Victims also reported spending an average of 60 hours, or 300 million hours collectively, to repair the damage inflicted by identity predators.

But, apart from its devastating financial impact, identity theft has a much darker side. What makes identity theft uniquely dangerous is that it is an enabling crime -- one that facilitates other types of crimes. Victims of identity theft have reported that criminals used their names to obtain employment, purchase firearms, file fraudulent tax returns, obtain government benefits, file for bankruptcy, and even coordinate terrorist activities, among other things.

PROMISCUOUS USE OF THE SSN

The root of the problem lies within the lax information sharing practices of financial institutions, merchants, credit bureaus, universities, student loan administrators, and government agencies at every level that maintain vast databases containing sensitive consumer information.

And, perhaps the most sensitive piece of information freely roaming the marketplace is the Social Security Number ("SSN"). SSNs play a crucial role in identity theft because they are not only a unique, nine-digit national identifier, but also an authenticator. This means that some businesses (like hospitals or student loan administrators) use it as a record locator or a master identifier to associate and reference records. Other businesses (like financial institutions) use it for authentication -- the process of proving a person's identity.

However, serious security problems arise in any system that relies so heavily on a single device as both an identifier and an authenticator. Even with such an over-dependence on this nine-digit number, no single federal law regulates how SSNs are used in the private sector. This would explain why so many entities routinely use the SSN as a data management tool to run their day-to-day operations, and why private companies often deny anyone credit, service or membership for refusing to furnish their SSN.

The result is an extremely vulnerable system that puts the entire burden on the consumer. With no power to control how their SSN is kept, used or distributed, consumers are left to simply sit-and-wait for an identity thief to strike. For this reason, the SSN is the key identifier criminals seek to obtain to hijack the lives of their victims.

IMPORTANT STEPS TO PREVENT IDENTITY THEFT

Needless to say, enhanced penalties for identity thieves is certainly a step in the right direction. But more must be done to prevent identity theft before it ever happens.

For one, putting a stop to the promiscuous use of SSN information can significantly help in reducing identity theft incidents. Given the alarming trends in identity theft schemes through SSN misuse, Congress should strive to limit availability of the SSN generally and to induce businesses to rely on alternative identifiers.

One way to force businesses to use alternative identifiers would be prohibiting private companies from denying goods or services to anyone unwilling to furnish their SSN, and prohibit public and private entities - such as universities or student loan administrators -- from using the SSN as their primary account number. This is essential to any sincere stab at reform.

Second, consumers have a right to know when databases containing sensitive personal data about them have been compromised. Historically, few entities voluntarily notify consumers when information systems are breached, and of the ones who do, few bother to help them through the process of cleaning up the mess caused by the security breach. This is a real concern.

Finally, credit reporting agencies -- which are currently liable only when they fail to follow "reasonable" procedures to ensure maximum possible accuracy -- should be made strictly liable for attributing the transactions of identity thieves to their innocent victims.

Our current system offers few incentives for credit bureaus to take affirmative steps to help

victims of fraud -- before or after it occurs.

For the victims, the result is that they are wronged twice: once by the thief; the other by the system. This can change if credit reporting agencies were made directly liable to victims for misreporting financial data *after* an alert is posted.

Overall, consumers stand to benefit from the tough new penalties facing identity thieves. With guaranteed prison terms, one can only hope that deterrence will play a key role.

But there is still plenty of room for improvement. Existing lax information sharing practices, coupled with our over-dependence on the SSN, leave consumers in a vulnerable position. By taking appropriate measures to address these obvious vulnerabilities, U.S. lawmakers can significantly thwart the continued growth of identity theft.

At the end of the day, prevention is far more effective than even toughest *after-the-fact* penalty.

Harry A. Valetk is a former trial attorney with the U.S. Department of Justice in New York City. He is an adjunct assistant professor at the Bernard M. Baruch College, Zicklin School of Business, and the chief legal officer of WiredSafety.org. He writes regularly on identity theft, privacy protections, and other consumer safety issues. Email: harry@valetk.com