NEWSLETTER

Identity Theft 911®

VOLUME 5
ISSUE 12
DECEMBER
2008

AMERICA'S LEADING IDENTITY MANAGEMENT AND EDUCATION SOURCE

THIS MONTH'S TOPIC...

The Perfect Storm

Why the New Administration Cannot Ignore Identity Theft

Notes from our Chairman, Adam K. Levin

As numerous industries and businesses implode and Americans lose their jobs and homes, it's clear that the incoming Obama administration faces a mountain of challenges, one in which identity theft is likely not considered top priority. Should we be concerned? Absolutely. This is why: We have the makings of the perfect storm. As more organizations face budget constraints, securing sensitive personal data becomes less of a priority and law enforcement has potentially fewer resources to catch criminals; more people in need could turn to identity theft to survive; and more Americans are in too precarious a financial state to adequately weather any measure of fraud.

This month, in "A Challenge to the President," three experts tell us what the Obama administration must do to better fight identity theft. And the editorial, "The Threat We Ignore at Our Peril," further makes the case for why the Obama administration must take aggressive action to help prevent identity theft from reaching Category 5 proportions.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: newsletter@identitytheft911.com

THE ECONOMY IS STAGGERING. IDENTITY THEFT WILL LIKELY ACCELERATE. WHAT THE OBAMA ADMINISTRATION NEEDS TO DO.

Not since Franklin Delano Roosevelt inherited the Great Depression in 1933 has a new U.S. president faced such trying economic circumstances. The challenges are severe: among them, two wars eating up the federal budget, unprecedented corporate bailouts and staggering job losses. If past trends provide any indication, this could bode poorly for U.S. crime rates, which some sociologists believe will increase in response to the nation's economic ailments. But while the relationship between the economy and criminal trends is subject to debate, few researchers expect a drop in rates of identity theft any time soon. For years, the crime has been on the rise. The new FTC-imposed security requirements for businesses, the "Red Flag Rules," designed to help detect, prevent and mitigate occurrences of identity theft, become effective in May, but their impact remains to be seen. So as non-profit groups, private businesses and law enforcement agencies providing identity theft assistance enter this new year, they're looking to the new administration for leadership. The federal government can play a prominent role in the fight against identity theft, with sweeping strokes of policy that can affect entire industries and the law.

We spoke to three thought leaders who've studied the identity theft issue about what they believe the Obama administration could do in 2009 to fight identity theft.

HERE ARE THEIR IDEAS...

JAY FOLEY
IDENTITY THEFT RESOURCE CENTER

Through the non-profit organization he runs with his wife, Linda, Jay Foley has been studying the identity theft issue for more than a decade. Over the course of these years, he's witnessed the victimization of two groups that really, if you think about it, would appear to be unlikely targets.

The first group is children. The second: the deceased.

Yet these demographic groups, neither of which would have any ostensible use for credit, are routinely hit: kids barely old enough for arithmetic signed up for credit card accounts; deed transfers in a deceased person's hand. The stories are absurd. Funny the government hasn't figured out an effective way to curb the problem. Can it?

Let's start with kids. One of the reasons it's comparatively easy to open new accounts in a child's name is that a child typically has no credit report to begin with, so there's no record to which an identity thief must conform or even consider; the thief gets to start from scratch, using a child's Social Security number, birth date and contact information pulled from his imagination. Foley's proposal: Preemptively create a record for all children under the age of 17 years, 10 months of age and house it in a digital repository. Foley even already has a name: the "1710 database." The database would contain the name, Social Security number and month/year of birth of every child. Potential creditors would check it when applications are received.

Foley says, "The screening process would eliminate a large percentage of the fraud that goes on in the United States today. Utility providers are hit by identity theft and fraud on a regular basis because mom and dad…didn't pay their bill. Now they're ducking out and are going to set up utility services in junior's name. [The 1710 database] would eliminate an awful lot of that nonsense."

To alleviate potential concerns from privacy advocates, Foley points out that as the database wouldn't include addresses, it would have no marketing value. "It's provided only to and for a specific purpose. It's going to eliminate an awful lot of garbage," he says.

As for the deceased, Foley has an idea that may help put an end to their identity resurrections. Both the problem and the solution lie in the Social Security Administration's Death Index, a database made public under the Freedom of Information Act through the Department of Commerce (one organization, the Provo, Utah-based Rootsweb, offers free access to the index online).

The index is intended to provide businesses with evidence that a person is, well, deceased. And businesses shouldn't extend credit to deceased people. The problem is that not all deceased people, whose deaths are typically filed with state health departments, are actually listed in the index, Foley says. "There's nothing that mandates the state to turn it over to the feds." The administration is notified of deaths, and the registry thus updated, when deaths are reported in regard to Social Security benefits (those that need to be stopped due to the death, or those claimed by a spouse), or when military burial benefits are requested, but this leaves too many loopholes nonetheless. Foley wants to see an automated system that ensures all deaths wind up recorded in the registry, in real time.

Finally, Foley would like to see a national registry of identity theft victims, accessible by police, which would prevent innocent people from being hauled off to jail for the crimes committed by scammers using their identity. Such a protocol could be integrated into the National Crime Information Center, a computerized index of criminal data currently used by law enforcement. That way, victims of identity theft don't have to "spend several days, several weeks…waiting for somebody to figure out you've got the wrong guy," Foley says.

PAM DIXON
WORLD PRIVACY FORUM

As if dealing with collection agencies, creditors, credit reporting agencies and law enforcement weren't bad enough, identity theft victims face yet more bureaucracy when dealing with the federal government. Stolen passport? Call the Department of State. Your mail's been stolen? Call the U.S. Postal Service. You suspect someone's been using your Social Security number for illegal purposes like employment? Call the Social Security Administration. What if someone uses your personal identifying information to obtain medical care? That's a call for the Department of Health and Human Services. And, oh yeah—don't forget to report the crimes to the Federal Trade Commission.

"Identity theft is a multi-issue problem," says Pam Dixon, Executive Director of the World Privacy Forum. "It makes sense not to split this crime up into sectors… It doesn't make sense for the consumer." Dixon suggests centralizing control of all identity theft-related issues with the FTC, which already maintains the federal government's identity theft statistics. "That's where the identity theft expertise is, that's where the identity theft staff is and the long term commitment to fighting identity theft," Dixon says. "There's no reason, at this point in time, not to make a decision to have the FTC own this issue. They should really be given any appropriate authority they need to take care of consumers in this area."

And should Dixon's vision of the FTC as central identity theft authority come to pass, one of its inaugural responsibilities under an Obama administration should be the creation of a repository of information on all organizational data breaches in America, accessible to businesses, consumers and law enforcement organizations alike. Of course, mandating the disclosure of data breaches to this centralized authority would require an act of Congress—data breach disclosure laws have traditionally been left up to the states—but Dixon says such an act is needed due to the paucity of accurate data breach information currently available.

The handful of small, non-profit groups that track data breaches have done a "heroic job," Dixon says, but they get their information not from organizations themselves but from secondary sources. "I do think the Obama administration needs to step up to the plate with strong, consumer-centric data breach legislation that doesn't require harm, for example, for a trigger," she says, meaning businesses should not be free to choose whether to disclose breaches based on perceived risk, as is allowed in some states. The ideal system: "If there's a breach, it gets reported."

One last thing: As the government considers policies regarding the sharing of electronic health care information, it needs to empower patients—first by giving them a choice whether they want their information shared beyond their immediate doctor, Dixon says, and second, by letting patients know who has accessed their medical records. "With health care privacy, it is not the outside hackers that cause the problem—it's insiders that are accessing the records," Dixon says. That's why she's calling on the Obama administration to support the idea of a digital "audit trail" accessible by patients, a system under which patients could see everyone who has accessed their records—not just those outside the health care system, but insiders as well. "We need to have 21st Century rights to go with 21st Century health care," Dixon says. "This fight is coming. You watch."

CHRIS HOOFNAGLE
BERKELEY CENTER FOR LAW AND TECHNOLOGY

I have a pretty simple answer," Chris Hoofnagle says when asked how the Obama administration could play a role in the battle against identity theft. "Identity theft prevention and remediation has focused on education of victims and prosecution of offenders. What we've left out are the companies in the middle—the companies that make credit offers to imposters." Cell phone companies, credit card companies—any organization that extends credit to consumers—these are, after all, the unwitting enablers of many identity theft crimes. And this, says the senior fellow for the Samuelson Law, Technology & Public Policy Clinic at the University of Berkeley, is a matter that ought to be taken on by federal regulators.

In February 2008, Hoofnagle put together a study on the rates of identity theft reported by individual financial institutions and other credit-extending entities like major wireless service providers. It was an admittedly imperfect study, its findings hindered by the inherently limited set of data with which he had to work—a three-month sampling of reports voluntarily submitted by consumers to the FTC for the year 2006. But as important as the findings themselves was the message Hoofnagle was hoping to send to the consumers, lawmakers and financial companies—that greater transparency, though sure to be contested by the companies upon which it would impose its mandates, would come to be a winning proposition for all parties.

Consumers would be empowered to make choices based on organizations' fraud prevention records. Competitive pressures, meanwhile, would force businesses to step up and ultimately cut back on rates of fraud-related losses. At least this is as the consumer activist and scholar sees it. What he hopes for in an Obama administration is a codified mandate requiring businesses to share information on rates of identity-related fraud. "It would be in their best interest to do this," Hoofnagle says. "It's a bitter pill to swallow, but in the long term would reduce fraud."

The Threat We Ignore at Our Peril

Identity theft poses greater devastation in bad economic times

A crisis is an opportunity riding the dangerous wind.

During this time of financial tumult, the familiar Chinese proverb bears repeating. The opportunity, of course, is that of the Obama administration implementing its platform of "change"—through policies that help create jobs and foster trade. But why stop there? As too many Americans edge ever closer to the brink of financial ruin, creating a plan to improve consumer financial security is an obvious lockstep strategy. Specifically, the Obama administration must take the issue of identity theft seriously, as so many of us are in such a tenuous financial situation that even one so-called minor instance of fraud committed against us could deal the final devastating blow.

If you look at identity theft statistics, you'll see there is no shortage of need for a comprehensive strategy to fight the crime. Federal Trade Commission complaint data published in February 2008 indicated that identity theft complaints to be at an all-time high. Observations from law enforcement officers, prosecutors and nonprofit organizations that study the identity theft problem, meanwhile, bear the same bleak message—that the mushroom cloud of identity theft is rising and ever-growing.

The ailing economy is but an accelerant. As Richard Rosenfeld, a sociologist at University of Missouri-St. Louis, recently observed in *The New York Times*, "Every recession since the late '50s has been associated with an increase in crime and, in particular, property crime and robbery, which would be most responsive to changes in economic conditions." Because identity theft is relatively easy to commit—the ultimate lazy man's (or woman's) crime in which the perpetrator almost never comes face-to-face with the victim—it would seem to be an attractive alternative to good old-fashioned breaking and entering. The Identity Theft Assistance Center, a nonprofit consortium of financial services companies, has voiced concerns about "hard-pressed consumers" turning to fraud and worries about a recession "forc(ing) state and local governments to cut their budgets, law enforcement agencies could be asked to do more with less," according to a recent statement.

Meanwhile, cyber-crime continues to grow and evolve—its tentacles extending from and around all reaches of the globe. Speaking with *Forbes* magazine, Gartner analyst Avivah Litan warned back in November of a spike in fraud related to the use of stolen data. She claimed some pretty good sources: Gartner's own banking clients. And here's the kicker: Litan proposed that the attacks were the handiwork of thousands of IT workers who had recently found themselves jobless "with the technical abilities needed to steal data or perpetrate fraud along with specific knowledge of their former employer's IT systems," according to *Forbes*. "In times like these, people need the cash," the magazine quoted Litan. "You have disgruntled IT

employees that leave companies, take customer records with them to sell them on the black market."

Bottom line: If what we've been reading is true, we are facing a legion of new criminals, and at this point we're woefully under-educated, under-resourced and out-gunned in the war against them. The good news? While the Obama administration may not hold the magical universal cure to this labyrinthine problem, it does have an unprecedented opportunity to effect sorely needed change at the highest level of government.

During the primary campaign season, Obama put forth a Technology and Innovation Plan (opens in .pdf) that laid out some high-level ideas on how problems of identity-related fraud might be tackled. The highlights included proposals to:

- Provide "robust protection against misuses of particularly sensitive kinds of information, such as e-health records and location data that do not fit comfortably within sector-specific privacy laws."
- Implement restrictions on how information in "powerful databases containing information on Americans that are necessary tools in the fight against terrorism" can be used. He also would enact measures to verify how the information actually has been used.
- Increase the Federal Trade Commission's enforcement budget and step up international cooperation to track down cyber-criminals, thus enabling U.S. law enforcement to better prevent and punish "spam, spyware, telemarketing and phishing intrusions into the privacy of American homes and computers."

Those are good enough ideas—especially the parts about protecting e-health records and going after cyber-crooks overseas. But where should the new president begin? Let's start with what the Obama administration *shouldn't* do. It shouldn't support Congressional efforts that would undermine hard-earned state statutes designed to protect consumer interests. In 2006, for example, The Financial Data Protection Act introduced by Rep. Steve LaTourette (R-OH), would have preempted data breach and credit freeze laws passed by various state legislatures. Fortunately, that bill never made it out of committee. Many states have enacted and implemented, and will likely continue to enact and implement, strong consumer protections. Their efforts shouldn't be negated with a broad legislative brushstroke.

Here's another important should-not: The Obama administration should not allow federal agencies to treat sensitive consumer data like ordinary office supplies. A January 2008 report from the Government Accountability Office noted that between 2003 and 2006, 19 federal agencies had reported at least one compromise of personal identifying information that could expose individuals to identity theft. The Office of Management and Budget responded with strong security mandates for all federal agencies, including those requiring data encryption, but even by July 2008, many had been woefully slow to respond. During a 2006 Senate hearing on the Department of Veterans Affairs data breach that resulted in the loss of 28.6 million veterans' Social Security numbers, then-Senator Barack Obama noted that "The system is so poorly designed that one employee can compromise the whole thing." It is imperative that under the Obama administration, the changes recommended during the previous administration are heeded by all agencies, all the time.

Those are a few things President Obama shouldn't do, but what about the thornier question of where to start? If there's a common thread to be found in the recommendations of the identity theft experts consulted for this month's newsletter, it's that of intelligence. We need to be able to pool crime data collected by disparate law enforcement, private and government agencies in order to provide a more timely and complete snapshot of the identity theft problem—and that requires significant funding and organization. Streamlining, cooperation and focus will also need to be emphasized in federal law enforcement. Among the 31 recommendations of the President's Identity Theft Task Force, an assemblage of representatives from 17 federal agencies convened by the Bush Administration 2006, was a suggestion for the establishment of a "national identity theft law enforcement center." This seems a reasonable goal, and perhaps one that could be coordinated along with Dixon's suggestion that the FTC be the go-to agency for victims.

As conversations with Jay Foley, Pam Dixon and Chris Hoofnagle attest, there is no shortage of ideas as to how we may assert greater control over the identity theft pandemic. Now it's up to the new president, as a great listener and mediator, to bring all voices to the table and apply to the identity theft problem that simple yet profoundly important ideal we heard about so much in the campaign season: Change. ■