Outside Counsel

Outside Counsel

Outside Counsel

New Bills Address Identity Theft

New Bills Address Identity Theft
By Harry A. Valetk
New York Law Journal

As part of the President's Homeland Defense initiative, several government agencies are working together to protect the nation from future acts of terrorism. However, Americans may have reason to worry about an existing vulnerability that is even closer to home: identity theft.

Identity theft is currently the nation's fastest-growing white-collar crime, victimizing an alarming 500,000 Americans each year.[1]† At the heart of the problem is our cultural reliance on using the Social Security number (SSN) as the primary way of identifying individuals.

Given its universal bearing in financial transactions, overuse by universities as a primary identification number, and its unfettered power for creating identities in the Information Age, the SSN today is a valuable asset that is too often subject to abuse. Indeed, in the wake of the World Trade Center and Pentagon attacks, identity theft has become an even greater concern after investigators learned that several hijackers used questionable means of identification to carry out their sinister plot.

As it now stands, authorities believe that our current identity information exchange system has many holes. As the de facto

national identifier, the SSN is exposing a growing number of students, consumers, and patients to greater risks online, where many share sensitive information about themselves, believing that current encryption technology and existing privacy policies are enough to guard against fraudulent schemes.

In universities around the country, for example, students must often disclose their SSN to register for classes, purchase books, and submit term papers or final exams.

But, our SSN dependency comes at a cost. In March, investigators arrested Abraham Abdallah, the Brooklyn busboy turned cyber-thief, just before he and an accomplice could steal $100 million by assuming the identities of Steven Spielberg, Oprah Winfrey, Martha Stewart, and many others.

Testifying before the Subcommittee on Social Security in May, New York City Detective Michael Fabozzi, one of the lead investigators in the Abdallah case, pointed out that the present system is not just vulnerable, but also leaves victims to fend for themselves trying to clear their good name.[2]† For most identity theft victims, it could take about two years to clear their credit history.

However, financial loss is not the only potential threat. For those with ulterior motives, the existing vulnerabilities in our system could be exploited to carry out "criminal identity theft," in which a perpetrator uses a stolen identity to commit a crime or avoid detection when he or she is arrested. Harrowed with grief and anxiety that someone used their good name to commit a crime, victims of criminal identity theft also face the possibility of arrest, followed by the daunting task of expunging criminal records.

Needless to say, our current dilemma is a complicated one with no simple solution. However, a main concern for consumer advocacy groups and government officials is that no federal law governs or even limits the use or disclosure of an individual's SSN among private entities. Although fraudulently using an individual's identity information is a crime,[3]† the after-the-fact approach currently in place does little to protect consumers from identity theft before it occurs.

What Can Be Done?

In practice, most preventive measures available are - at best - illusory because consumers have no actual control over how their SSN is kept, used, or distributed. Even more invasive, private entities are free to deny anyone credit, service, or membership for refusing to furnish their SSN.

Living proof of the identity theft prevention fallacy is a Maryland resident that fell victim to identity theft, despite her precautionary practice of shredding sensitive financial statements and reviewing her credit report annually. In her case, her identity predator worked for a business that maintained HMO databases and was able to access her SSN and date of birth. Using only these two pieces of information, the perpetrator obtained over $36,000 in goods, while adversely affecting the victim's ability to refinance her home and obtain credit.

More recently, the U.S. Supreme Court decided a case involving a

patient that fell victim to identity theft after her doctor's former receptionist stole her SSN information from an in-take form, and opened several credit accounts.[4]† In that case, the Court reversed the U.S. Court of Appeals for the Ninth Circuit, and held that the two-year statute of limitations to bring an action under the Fair Credit Reporting Act begins when the alleged wrongful disclosure occurs, not when an individual discovered the wrongful disclosure.

Ironically, and contrary to popular belief, the Social Security Administration has no power to control how private entities use their account numbers, even though the SSN was originally created in 1936 solely for tracking workers' Social Security earnings records.[5]†

Sooner or later, this must be changed. Before the Sept. 11 attacks, both the House and the Senate proposed several bills to regulate how SSN information is used, and hold private entities accountable when SSNs are sold without the number holder's consent. But, like so many other legislative agendas, this too was put aside and may never see the light of day.

Still, some experts believe that the proposed identity protection legislation could gain momentum as part of the Government's new technological vulnerability review. To understand the proposed statutes and their likely impact on marketplace practices, we can review three bills presently before Congress.

Congressional Proposals

The Social Security Number Privacy and Identity Theft Act of 2001 (SSNPITA" is a comprehensive bill aimed at preventing fraudulent misuse of the SSN in both the public and private sectors.[6]† Simultaneously proposed in the House by Representative E. Clay Shaw, Jr., R-Fla., and in the Senate by Senator Jim Bunning, R-Ky., SSNPITA would address existing vulnerabilities in the present system by prohibiting the following activities:

• sale, purchase, or display of SSNs by governmental agencies;

• sale, purchase, or display of SSNs by private companies.

• appearance of SSNs on driver's licenses or motor vehicle registrations;

• governmental agencies from using SSNs as numbers shown on identification cards;

• governmental agencies and private contractors from employing prisoners in jobs with access to SSN information; and

• anyone from obtaining an individual's SSN to locate or identify the number holder with the intent to injure, harm, or misuse his or her identity information.

SSPITA would also require that all credit header information containing SSN information be treated as confidential information subject to the same protections as a full consumer report. Although SSNPITA would impose new criminal and civil penalties of up to

$5,000 for each violation involving SSN misuse, the bill has its shortcomings.

Particularly, SSNPITA would not prevent private companies from denying goods or services to anyone unwilling to furnish their SSN, nor would it prevent entities - like universities or student loan administrators - from using the SSN as their primary account number.

Another proposal is the Social Security Number Misuse Prevention Act of 2001 (SSNMPA). SSNMPA was introduced on May 9th in the Senate by Senator Dianne Feinstein, D-Calif., to limit SSN misuse. [7]† To that end, SSNMPA prohibits the following activities:

• public display of an individual's SSN without the number holder's consent;

• Federal, State, or local agencies from displaying SSN information on any checks issued;

• display of the SSN on driver's licenses or motor vehicle registration;

• sale or purchase of an individual's SSN without the number holder's consent;

• governmental agencies and private contractors from employing prisoners in jobs with access to SSN information; and

• anyone from obtaining an individual's SSN to locate or identify the number holder with the intent to injure, harm, or misuse his or her identity information.

In a key provision that fosters identity protection, SSNMPA would also forbid any commercial entity from denying goods or services to any individual that refuses to furnish his or her SSN. Aggrieved individuals would have a right of action in federal court to recover damages ranging from $2,500 to $10,000 and authorities could levy fines of up to $50,000 against frequent violators.

Blocking Sales of SSNs

Employing a more limited approach, the Personal Information Privacy Act of 2001 (PIPA) was proposed by Representative Gerald Kleczka, D-Wis., to protect SSN information. [8]† PIPA would impose the following provisions:

• require all credit header information containing SSN information to be treated as confidential information under the Fair Credit Reporting Act;

• prohibit anyone from buying or selling an individual's SSN without the number holder's written consent;

• prohibit anyone from using the SSN for identification purposes without number holder's written consent; and

• define "an unfair or deceptive act" under the Federal Trade

Commission Act to include any person who refuses to do business with someone because that individual will not consent to disclosing their SSN.

For consent to exist, the number holder must be informed about all the purposes for which the number will be utilized and the persons to whom the number will be known. Finally, PIPA would give individuals standing to recover up to $50,000 in damages, and SSA the power to impose a $25,000 fine for each violation or up to $500,000 for frequent violators.

What Should We Expect?

Regardless of which bill is ultimately enacted, protecting our identities from petty thieves - or international terrorists - is necessarily an essential component of any homeland defense strategy. To better serve Americans, new legislation addressing identity theft should be simple, based on fair information practices, and include few exceptions or loopholes. At the same time, any new law should also build on - not weaken or overlap with - existing privacy protections, including those of the Privacy Act and the Gramm-Leach-Bliley Act.

Above all, new legislation should limit SSN use to only those purposes that benefit number holders, not information brokers, mass marketers, or other entrepreneurs that use it as a convenient means of identification or carelessly expose it to misuse by making it available for a fee. Harry A. Valetk *is an assistant regional counsel for the Social Security Administration in New York. The opinions expressed in this article are the author's, not those of the Administration.*

FootNotes: [1]

††† Adam Cohen, "Internet Insecurity," Time, July 2, 2001, at 46. [2]

††† Protecting Privacy and Preventing Misuse of Soc. Sec. Numbers, Before the Subcomm. on Soc. Sec. of the Comm. on Ways and Means H.R., 107th Cong. (2001) (testimony of Michael Fabozzi). [3]

††† 42 U.S.C. §408(a)(6)-(8) (making it a felony to use or disclose a social security number for fraudulent purposes); see also, Internet False Identification Prevention Act of 2000, Pub. L. No. 106-578, 114 Stat 3075 (strengthening the enforcement of Federal statutes relating to false identification); Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat 3007 (making it unlawful for someone to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or is a felony under State or local law"). [4]

††† TRW v. Andrews, -U.S.-, 2001 WL 1401902 (Nov. 13, 2001). [5]

††† Under the Privacy Act, however, some restrictions exist on the use of an individual's SSN by governmental agencies that make it "unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number," unless otherwise required by statute. 5 U.S.C. §552a note

(Disclosure of Social Security Number); see also Privacy Act, Section 7 (a)(1). [6]

††† Social Security Number Privacy and Identity Theft Act, S. 1014, H.R. 2036, 107th Cong. (2001). [7]

††† Social Security Number Misuse Prevention Act, S.848., 107th Cong. (2001). [8]

††† Personal Information Privacy Act, H.R. 1478, 107th Cong. (2001).

Date Received: *December 31, 2001*