ELECTRONIC PRIVACY INFORMATION CENTER

Statement of the Electronic Privacy Information Center to
Maryland Attorney General Identity Theft Forum
Baltimore, MD
November 21, 2005

Dear Attorney General Curran,

Thank you for convening this forum on identity theft and for soliciting comment from the Electronic Privacy Information Center (EPIC). EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

We believe that individuals need to have more control over their credit report in order to curb identity theft. Specifically, individuals should be able to "freeze" their credit report. A frozen credit report is inaccessible to credit grantors. Credit grantors will not open a new account without a credit report. Therefore, by allowing consumers to have more control and freeze their reports, they can stop identity theft.

In the identity theft debate, there has not been enough consideration of allowing individuals to control their own data to prevent the crime. Currently, access to credit reports is controlled by consumer reporting agencies, companies that make money by selling reports. Hundreds of thousands of "users" have access to the consumer reporting system and are able to obtain reports on anyone with just a few keystrokes. Under the current system, a huge network of businesses have total control over our most detailed financial information.

Giving individuals control over credit reports would check market forces that have flamed the identity theft problem. In the world of instant credit, credit grantors are under incredible competitive pressure to issue new accounts. This pressure makes it easy for even unsophisticated criminals to gain access to new accounts in others' names. In fact, lax practices so permeate the current system that credit cards have been issued to dogs and babies.

Federal legislative efforts to address identity theft have ignored individuals' lack of control and the mounting evidence that instant credit contributes to the crime. Federal law allows individuals to file fraud alerts and identity theft warrants, but these measures are remedial and are employed after the crime has occurred. Congress has criminalized identity theft and heightened penalties. None of this has served to prevent the crime.

Meanwhile, the financial services industry has begun to "blame the victim" for identity theft. They argue that in a large majority of cases, roommates, family members, and others close to the victim most often commit the crime. However, only about half of identity theft victims even

know how their identity was stolen.[1] Only 26% know the actual identity of the thief, and in those cases, 35% of the time, the impostor was a family member.[2] This crime remains one where most people do not know how it was committed nor who committed it. But the financial services industry wants to blame the victim in order to maintain the status quo, and to shift the focus from away from their own practices. Blaming the victim distracts policymakers from the issue that needs to be addressed: individual control over credit reports.

Consumers need to be able to freeze their credit reports to prevent identity theft. Credit freeze is a sensible option that people should be able to choose to take. But because of market forces, it is a choice that consumer reporting agencies will not offer the public. Consumer reporting agencies want to decide for us how our personal information will be controlled.

Understanding the Roots of Identity Theft

Instant Credit Makes the Crime Easy to Commit

It is important to understand that much of the current scourge of identity theft is caused by irresponsible, lax credit granting procedures associated with instant credit. Grantors have flooded the market with "pre-screened" credit offers, pre-approved solicitations of credit made to individuals who meet certain criteria. These offers are sent in the mail, giving thieves the opportunity to intercept them and accept credit in the victim's name.[3] Once credit is granted, the thief changes the address on the account in order to obtain the physical card and to prevent the victim from learning of the fraud.[4] The industry sends out billions of these pre-screened offers a year. It 1998, it was reported that 3.4 billion were sent.[5] In 2003, the number increased to an estimated 5 billion.[6]

Competition also drives grantors to quickly extend credit. Once a consumer (or impostor) expresses acceptance of a credit offer, issuers approve the transaction with great speed. Experian, one of the "big three" consumer reporting agencies, performs in this task in a "magic

---

[1] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 28, Sept. 2003, available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[2] "35% of the 26% of victims who knew the identity (or, in other words, 9% of all victims) said a family member or relative was the person responsible for misusing their personal information…23% of the 26% of all victims who knew the identity of the thief (or 6% of all victims) said the person responsible was someone who worked at a company or financial institution that had access to the victim's personal information… Of the 26% who knew the identity of the person who took their information, 18% said the thief was a friend, neighbor, or in-home employee, while 16% said the thief was a complete stranger, but the victim later became aware of the thief's identity. (These figures represent 5% and 4% of all victims respectively.) *Id*. at 28-29.

[3] *Identity crises -- millions of Americans paying price*, CHI. TRIBUNE, Sept. 11, 2003, p2.

[4] *Id*.

[5] *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, Hearing Before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, Jul. 12, 2000 (testimony of Beth Givens, Director, Privacy Rights Clearinghouse) (*citing* Edmund Sanders, *Charges are flying over credit card pitches*, L.A. TIMES, Jun. 15, 1999, p. D-1), available at http://www.privacyrights.org/ar/id_theft.htm.

[6] Rob Reuteman, *Statistics Sum Up Our Past, Augur Our Future*, ROCKY MOUNTAIN NEWS, Sept. 27, 2003, p 2C; Robert O'Harrow, *Identity Crisis; Meet Michael Berry: political activist, cancer survivor, creditor's dream. Meet Michael Berry: scam artist, killer, the real Michael Berry's worst nightmare*, WASH. POST MAG., Aug. 10, 2003, p W14.

two seconds."[7] For instance, in a scenario published in an Experian white paper on "Customer Data Integration," an individual receives a line of credit in two seconds after only supplying his name and address.[8] Such a quick response heightens the damage to business and victims alike, because thieves will generally make many applications for new credit in hopes that a fraction of them will be granted.

Adam Smith, a political columnist with the St. Petersburg Times recently related in a story about his own experience with identity theft came to the conclusion that the credit industry and instant credit exacerbates the crime:

> The experience already had taught me that the credit industry makes it too easy for thieves to plunder other people's credit and too hard for victims to clear their names. Talking to [Smith's identity thief] Shad Fish, I learned it's worse than I thought.
>
> […]
>
> Think of Mr. Fish the next time a cashier encourages you to open a new credit account and get an instant discount. Retailers love anything that entices people to make impulse purchases. My identity thief loved it, too.
>
> "They make it so easy with the instant credit system. It blew my mind how easy it was when I first started. All you have to do is fill out a form, hand them an ID and instantly $20,000 becomes available. Then they want you to spend that $20,000 immediately." [Fish said.][9]

Similarly, Philadelphia Inquirer columnist Jeff Gelles concluded:

> The system that makes easy credit possible also fuels identity theft. And since the Big Three [Experian, Equifax, and Trans Union] have learned how to profit from fears of identity theft, they have little incentive to fix the underlying problem.[10]

Identity Verification is Inadequate

Another factor in lax issuance is that credit grantors do not have adequate standards for verifying the true identity of credit applicants. Credit issuers sometimes open tradelines to individuals who leave obvious errors on the application, such as incorrect dates of birth or fudged Social Security Numbers. Identity theft expert Beth Givens has argued that many incidences of identity

---

[7] EXPERIAN, INC., CUSTOMER DATA INTEGRATION: THE ESSENTIAL LINK FOR CUSTOMER RELATIONSHIP MANAGEMENT WHITE PAPER 15, 2000, available at http://www.experian.com/whitepapers/cdi_white_paper.pdf.
[8] *Id*.
[9] Adam Smith, *Ruining my credit was easy, thief says, Armed with my information, an impostor racked up $45,000 in charges. Creditors are fighting a proposed fix*, ST. PETERSBURG TIMES, Oct. 23, 2005, available at http://www.sptimes.com/2005/10/23/Worldandnation/Ruining_my_credit_was.shtml.
[10] Jeff Gelles, *Whom to Blame for ID Theft*, PHILADELPHIA INQUIRER, Nov. 7, 2005, available at http://www.philly.com/mld/inquirer/business/13100168.htm.

theft could be prevented by simply requiring grantors to more carefully review credit applications for obviously incorrect personal information.[11]

Standards are so lax that even dogs are issued credit cards. Chase Manhattan issued a platinum Visa card to "Clifford J. Dawg" in 2004.[12] In this instance, the owner of the dog had signed up for a free e-mail account in his pet's name and later received a pre-approved offer of credit for "Clifford J. Dawg." The owner found this humorous and responded to the pre-approved offer, listing nine zeros for the dog's Social Security number, the "Pupperoni Factory" as employer, and "Pugsy Malone" as the mother's maiden name. The owner also wrote on the approval: "You are sending an application to a dog! Ha ha ha." The card arrived three weeks later.[13] Credit has been offered and issued to other dogs, including Monty, a Shih-Tzu who was extended a $24,600 credit line.[14]

The slip ups also occur with humans. Credit has been granted to children and babies and young teenagers.[15] These events suggest that the credit issuers are lax in their marketing and authentication efforts. It suggests that the applications are processed by a computer, and no human reviews them to prevent fraudulent or improper credit granting.

TRW Inc. v. Andrews illustrates the problems with poor standards for customer identification.[16] In that case, Adelaide Andrews visited a doctor's office in Santa Monica, California, and completed a new patient's information form that requested her name, birth date, and Social Security Number.[17] The doctor's receptionist, an unrelated woman named Andrea Andrews, copied the information and used Adelaide's Social Security Number and her own name to apply for credit in Las Vegas, Nevada. On four occasions, Trans Union released Adelaide's credit report because the Social Security Number, last name, and first initial matched. Once Trans Union released the credit reports, it made it possible for creditors to issue new tradelines. Three of the four creditors that obtained a credit report issued tradelines to the impostor based on Adelaide's file, despite the fact that the first name, birth date, and address did not match.[18]

There are many other cases where creditors issued new accounts to individuals who presented applications with obvious errors. For instance, in *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004), a phone company issued credit to an impostor who used the victim's name but a

---

[11] *Legislative Hearing on H.R. 2622, The Fair and Accurate Credit Transactions Act of 2003, Before the Committee on Financial Services*, Jul. 9, 2003 (testimony of Chris Jay Hoofnagle, Deputy Counsel, Electronic Privacy Information Center).
[12] *Dog Gets Carded*, WASH. TIMES (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC SAN DIEGO (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.
[13] *Id.*
[14] *Identity thieves feed on credit firms' lax practices*, USA TODAY, Sept. 12, 2003, p. 11A; Kevin Hoffman, *Lerner's Legacy: MBNA's customers wouldn't write such flattering obituaries*, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, *A Week in Bankruptcy Court*, ST. PETERSBURG TIMES, Mar. 18, 2002, p 8E.
[15] IDENTITY THEFT RESOURCE CENTER, FACT SHEET 120: IDENTITY THEFT AND CHILDREN, available at http://www.idtheftcenter.org/vg120.shtml.
[16] 534 U.S. 19 (2001); Erin Shoudt, *Identity theft: victims "cry out" for reform*, 52 Am. U. L. Rev. 339, 346-7 (2002).
[17] *Id.* at 23-25.
[18] *Id.*

slightly different Social Security Number. In *United States v. Peyton*, 353 F.3d 1080 (9th Cir. 2003), impostors obtained six American Express cards using the correct name and Social Security Numbers of victims but directed all six cards to be sent to the impostors' home. In *Aylward v. Fleet Bank*, 122 F.3d 616 (8th Cir. 1997), the bank issued two credit cards based on a matching name and Social Security Number but an incorrect address. In *Vazquez-Garcia v. Trans Union De P.R.*, Inc., 222 F. Supp. 2d 150 (D.P.R. 2002), an impostor successfully obtained credit with matching Social Security Number but incorrect date of birth and address. The address used by the impostor wasn't even in Puerto Rico. In *Dimezza v. First USA Bank, Inc*., 103 F. Supp. 2d 1296 (D.N.M. 2000), an impostor obtained credit with a Social Security Number match but incorrect address.

Consumers Need Control Over Credit Reports to Prevent Identity Theft

At the federal level, legislative and regulatory efforts to address the identity theft have centered on remedial measures, including the creation of "identity theft affidavits," which assist victims in reporting the crime to creditors and consumer reporting agencies.[19] Victims can also file "fraud alerts" to help deter creditors from giving an impostor a new line of credit. But these alerts are not filed until fraud is actually suspected, and a recent report found that creditors ignore fraud alerts in some identity theft cases.[20] These remedial measures do little to prevent identity theft. In fact, even formally criminalizing identity theft has not been effective in curbing its incidence.[21]

Because it is too easy for impostors to open new accounts in victim's names, and because existing protections are ineffective in preventing identity theft, we need to empower consumers to limit credit report availability. If individuals can prevent the release of their credit report, they can stop identity thieves from opening new accounts in their name.

Enabling consumers to freeze their credit would address the sloppy procedures driven by instant credit. A frozen system also solves a long-standing problem with authorized access to credit reports, the "impermissible pull." This occurs where someone with access to the consumer reporting system obtains a report on a consumer without a credit application or existing relationship with the consumer.

For credit freeze to work, it has to be easy for consumers to use. All individuals should be able to trigger a freeze (not just identity theft victims). There should also be a method for the individual to quickly thaw their report, so that individuals can take advantage of credit and employment opportunities.

---

[19] FEDERAL TRADE COMMISSION, IDENTITY THEFT AFFIDAVIT, at http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf.

[20] Linda & Jay Foley, IDENTITY THEFT: THE AFTERMATH 2004, 16, Sept. 2005, available at http://www.idtheftcenter.org/aftermath2004.pdf.

[21] Congress formally criminalized identity theft in 1998, but reports of the crime continue to rise. *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. Law. No. 105-318, 112 Stat. 3007 (Oct. 30, 1998); FEDERAL TRADE COMMISSION, OVERVIEW REPORT AND TIMELINE OF THE IDT PROGRAM, Figure 1, Sept. 2003, available at http://www.ftc.gov/os/2003/09/timelinereport.pdf. In 2004, Congress increased the penalties for using personal information in connection with fraud, terrorism, and numerous federal felonies. Identity Theft Penalty Enhancement Act, Pub. L. 108-275 (Jul. 15, 2004). It is unclear what effect the legislation will have.

Credit freeze can also be supplemented by additional protections against irresponsible credit granting. For instance, credit grantors should have to screen customers more carefully. In California, which has the highest standard, an instant credit grantor only has to match three identifiers from the application to the credit "header" on file at the consumer reporting agency.[22] However, this protection only applies when an individual applies for credit at a retailer.[23] Thus, Internet, telephone, and mail credit granting is not covered. Furthermore, the categories of information to be matched could probably be found in public records, the white pages, or other readily-available tools. The categories to be matched include "first and last name, month and date of birth, driver's license number, place of employment, current residence address, previous residence address, or social security number."[24] The California requirement is imperfect, but if strengthened to require 4 or 5 identifiers to match, identity theft would be more difficult to commit.

Finally, credit grantors should be liable for damages when negligent in issuing a new account to an impostor. Companies that issue credit cards to dogs, toddlers, and to identity thieves who can't even get the victim's address right share blame for the crime.

Conclusion

Identity theft is out of control because individuals have no control over their personal information. Instead, a vast network of businesses that make money from selling information are in control. Shifting control to the consumer by allowing the option of credit freeze will check the market forces that contribute to identity theft. Those who do not wish to freeze their credit are welcome to leave it in its current, vulnerable state.

A properly designed freeze with a quick-thaw procedure will allow even those who freeze their credit can take advantage of in-store specials and instant credit opportunities.

Respectfully submitted,

Chris Jay Hoofnagle
Senior Counsel
Electronic Privacy Information Center West Coast Office

[22] Cal. Civ. Code § 1785.14.
[23] Cal. Civ. Code § 1785.14(a)(1).
[24] *Id*.