



**SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC  
CENTER FOR CLINICAL EDUCATION**

CLINICAL PROFESSOR AND DIRECTOR  
Deirdre Mulligan  
(510) 642-0499  
dmulligan@law.berkeley.edu

SCHOOL OF LAW (BOALT HALL)  
BERKELEY, CALIFORNIA 94720-7200  
TELEPHONE (510) 643-4800  
FAX (510) 643-4625  
<http://www.law.berkeley.edu/academics/samuelson/>

[Submitted by email to [idmworkshop@ftc.gov](mailto:idmworkshop@ftc.gov)]

March 8, 2007

Federal Trade Commission  
Office of the Secretary  
Room H-135 (Annex N)  
600 Pennsylvania Avenue, N.W.,  
Washington, D.C. 20580

Re: Request to Participate in ID Workshop, P075402

Dear Commissioners,

The Samuelson Law, Technology & Public Policy Clinic requests to have Chris Hoofnagle participate as a panelist in the Commission's upcoming Proof Positive Workshop.

Based at the University of California's Boalt Hall School of Law, the Samuelson Clinic gives students hands-on training while providing a new voice for the public interest. The Clinic aims to serve as the public's voice in legal and regulatory disputes presently dominated by lobbyists and the government. The Clinic has provided legal advice and representation on issues of privacy (online, wireless communication, library and school Internet filtering, electronic voter records), free speech (Internet jurisdiction and enforcement of foreign judgments, inmate access to information originating on the Internet, library and school filtering, unsolicited email, online consumer complaints and information sharing, online publisher liability for third party content, publisher liability), copyright (term extensions, search engine liability for infringement, Digital Millennium Copyright Act, digital rights management technology), and open source issues (online licensing of creative content, liability issues).

Our request to participate is based on academic work performed on three issues critical to authentication and identity theft: the rise of "synthetic identity theft," the problem of

"negligent" credit granting, and the need for reporting by lending institutions on identity theft.

Financial services companies have long argued that privacy laws frustrate their efforts to fight fraud. However, our participation would focus on how credit granting policies and procedures of financial services companies contribute to the identity theft problem. We suspect, because of the rise of synthetic identity theft, that some grantors are not using all the tools already available to them to prevent the crime. Furthermore, many examples of "negligent" credit granting suggest that simple changes in procedure could curb incidence of the crime. Accordingly, individuals' privacy does not need to suffer in order to prevent identity theft.

We also wish to emphasize the need for lending institutions to reveal more data about identity theft. Currently, the publicly available data on identity theft come mainly from survey research. Methodologically, these survey polls of the public suffer from being both under and overinclusive in measuring the problem. One way to provide concrete data is to require lending institutions to publicly report figures on identity theft. Such public reporting will help identify the relative need for intervention and the likely efficacy of interventions.

### **Synthetic Identity Theft**

In synthetic identity theft cases, the impostor creates a new identity using some information from a victim that is enhanced with fabricated personal information.<sup>1</sup> For instance, the impostor may use a real Social Security number, but a falsified name and address. Since this synthetic identity is based on some real information, and sometimes supplemented with artfully created credit histories, it can be used to apply for new credit accounts.

A sophisticated example of the crime is well illustrated by a case brought by the U.S. Attorney for the District of Arizona in August 2006:<sup>2</sup> In the still-ongoing case, two men are charged with a variety of federal crimes for allegedly using real Social Security numbers from credit reports combined with fabricated names to apply for credit cards.<sup>3</sup>

---

<sup>1</sup> FDIC, PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT (Dec. 14, 2004), available at <http://www.fdic.gov/consumers/consumer/idtheftstudy/index.html>; Fred H. Cate, *Information Security Breaches and the Threat to Consumers* (Sept. 2005), available at [http://www.hunton.com/files/tbl\\_s47Details/FileUpload265/1280/Information\\_Security\\_Breaches.pdf](http://www.hunton.com/files/tbl_s47Details/FileUpload265/1280/Information_Security_Breaches.pdf).

<sup>2</sup> William Carlile, *Two Indicted in Credit-Card Scheme That Used SSNs From Credit Reports*, 5 Privacy & Security Law Report 1257, Sept. 11, 2006; Donald G. Aplin, *Privacy, Security Protection Will Remain Key Part of FTC's Agenda, Majoras Says*, 5 Privacy & Security Law Report 1552, Nov. 13, 2006.

<sup>3</sup> *US v. Rose et al*, CR06-0787PHK-JAT (VAM) (D. Az. 2006), *indictment filed Aug. 22, 2006*.

One of the men owned a small consumer reporting agency, and apparently has a high level of sophistication in credit practices.<sup>4</sup> The pair established credit histories for synthetic identities by reporting favorable payment information to consumer reporting agencies. In doing so, the synthetic identities appeared to be real people with a track record of paying bills. They then, it is alleged, obtained 250 credit cards from 15 banks, and charged \$760,000 to these synthetic identities.<sup>5</sup>

Below, from the indictment, it can be seen that a Social Security number assigned to a real person ("Haqqani Saifullah") was used to apply for a credit card for a synthetic identity ("Hanna Curin").<sup>6</sup>

Count	Date (on or about)	False Name	Amount of money obtained from use	Credit card #
1	05/02/2002	Hanna Curin (SSN 7483 assigned to Haqqani Saifullah)	\$3,481.00	Fleet #0519

The fact that a synthetic identity thief can use a fake name in combination with a real Social Security number to obtain credit cards sent to a mailbox not associated with the victim suggests that lending institutions are not authenticating the *identities* of credit applicants. It suggests that the Social Security number is being used alone as both identifier and authenticator. This has serious public policy implications. In the public policy debate, lending institutions oppose privacy legislation, arguing that increased privacy rights can prevent fraud prevention efforts.<sup>7</sup> But if lending institutions are only engaging in authentication of the Social Security number (ensuring that the number is issued to a live person, and that the credit applicant has a date of birth consistent with the number) rather than identity authentication (ensuring that the number is issued to the correct person), it means that lending institutions are not using all the tools available to them to prevent identity theft. Additional privacy laws will not harm their anti-fraud efforts, because they are not currently using already available information to authenticate the identities of credit applicants.

*Understanding synthetic identity theft is important, because it demonstrates problems in the credit authentication process. If we can understand why synthetic identity theft occurs—why an applicant with a fake name but a real Social security number can obtain credit—it will inform efforts to eliminate other forms of identity theft.*

<sup>4</sup> Rose, Indictment at 2.

<sup>5</sup> Rose, Indictment at 3-4.

<sup>6</sup> Rose, indictment at 5.

<sup>7</sup> Hjalma Johnson, *Banking and the Future of Financial Privacy: A Commitment to Our Customers*, American Bankers Association (Nov. 15, 1999), available at [http://www.aba.com/Press+Room/PR\\_Privacy\\_HJSpeech.htm](http://www.aba.com/Press+Room/PR_Privacy_HJSpeech.htm); AMERICAN BANKERS ASSOCIATION, *THE DEVASTATING EFFECT OF OPT-IN RESTRICTIONS* (n.d.), available at [http://www.aba.com/Industry+Issues/GR\\_PR\\_Opt-in.htm](http://www.aba.com/Industry+Issues/GR_PR_Opt-in.htm).

## Negligent Credit Granting: Privacy Shouldn't Suffer Because of Bad Policies

Identity theft is a reflection of business practices and policies. Instant credit opportunities and competition to obtain new customers drive some lenders to grant new accounts without adequately vetting the customer. Examples of mistakes in credit granting abound in the media, and bring into question whether more authentication tools are needed, because these problems should have been prevented from common sense procedures, such as verification of address, date of birth, etc.

- One consumer took an unsolicited credit card offer, ripped it up, reassembled it with tape, and then submitted it to a bank with a change of address. The bank issued the card, and even sent it to the different address, thus demonstrating that a thief could easily use even a torn-up offer for fraud.<sup>8</sup>
- Chase Manhattan bank issued a platinum visa card to "Clifford J. Dawg." 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.<sup>9</sup>
- Credit has been offered and issued to other dogs, including Monty, a Shih-Tzu who was extended a \$24,600 credit line.<sup>10</sup> It also has been granted to children and babies.<sup>11</sup>

In several lawsuits concerning identity theft, further examples of negligent credit granting have emerged:

- In *Vazquez-Garcia v. Trans Union de Puerto Rico*, Sears issued a credit card to an impostor who used the victim's Social Security number but wrong address and

---

<sup>8</sup> Bob Sullivan, *Even torn-up credit card applications aren't safe*, MSNBC, Mar. 14, 2006, available at [http://redtape.msnbc.com/2006/03/what\\_if\\_a\\_despe.html](http://redtape.msnbc.com/2006/03/what_if_a_despe.html).

<sup>9</sup> *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>.

<sup>10</sup> *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.

<sup>11</sup> IDENTITY THEFT RESOURCE CENTER, FACT SHEET 120: IDENTITY THEFT AND CHILDREN, available at <http://www.idtheftcenter.org/vg120.shtml>.

date of birth. The victim was a resident of Puerto Rico, but several cards were issued to an impostor using a Nevada address.<sup>12</sup>

- In *United States v. Peyton*, a criminal case, American Express issued six cards to impostors who used the victims' correct names and Social Security numbers but directed all six to be sent to the impostors' home.<sup>13</sup>
- In *Nelski v. Pelland*, Ameritech opened an account for an impostor who used the victim's name, but a different address and slightly different Social Security number.<sup>14</sup>
- In *Dimezza v. First USA Bank, Inc.*, First USA Bank issued a credit card to an impostor who used the victim's Social Security number but a different first name and address.<sup>15</sup>
- In *Alward v. Fleet Bank*, Fleet Bank issued two credit cards in the name of the victim to a New York address. The victim had never lived in that state.<sup>16</sup>
- In *Fritzhand v. Discover Financial Services*, Discover accepted a \$14,000 balance transfer from a fraudulently-obtained American Express account. Both accounts were opened with the victim's name but with a fictitious address.<sup>17</sup>
- In *Farley v. Williams & U.C. Lending*, a store line of credit and a Citibank platinum card were issued to an impostor using the victim's name and Social Security number but the impostor's home address.<sup>18</sup>
- In *Garay v. U.S. Bancorp*, a credit card with a \$20,000 limit was issued in the victim's name to an impostor who applied using the name of a business that had no Dun & Bradstreet Report.<sup>19</sup>

These anecdotal examples from news reports and litigation demonstrate that in at least some cases, fraud could have been avoided with common-sense changes in procedures. Privacy laws would not obstruct anti-fraud efforts in these cases, because simple tools long available to lending institutions, such as address verification databases, could have prevented the frauds.

### **Identity Theft Reporting**

In the last month, Javelin Strategy reported that 8.4 million Americans were victims of identity theft in the last year, Gartner put the number at 15 million, and the Federal Trade Commission observed that identity theft continues to be the top complaint received by the

---

<sup>12</sup> 222 F. Supp. 2d 150 (D.P.R. 2002).

<sup>13</sup> 353 F.3d 1080 (9th Cir. 2003).

<sup>14</sup> 2004 U.S. App. LEXIS 663 (6th Cir. 2004).

<sup>15</sup> 103 F. Supp. 2d 1296 (D.N.M. 2000).

<sup>16</sup> 22 F.3d 616 (8th Cir. 1997).

<sup>17</sup> 800 N.Y.S.2d 316 (New York Supreme Court, Nassau County 2005)

<sup>18</sup> 2005 U.S. Dist. LEXIS 38924 (W.D.N.Y. 2005).

<sup>19</sup> 303 F. Supp. 2d 299 (E.D.N.Y. 2004).

agency. Estimates in costs attributable to identity theft range from the tens of billions to \$279 billion.<sup>20</sup>

The publicly available data on identity theft come mainly from survey research. Methodologically, these survey polls of the public suffer from being both under and overinclusive in measuring the problem.

To identify proper interventions and appropriately allocate resources we need comprehensive, hard data on the scope and effect of identity theft. One way to provide concrete data is to require lending institutions to publicly report figures on identity theft. Such public reporting will help identify the relative need for intervention and the likely efficacy of interventions. These disclosures are necessary to provide a sound baseline for investment by businesses and action by regulators. They are also warranted because the public pays the price of identity theft directly when they are the victim, and indirectly through higher fees, interest rates, and because the losses are tax subsidized.

In the attached paper, I propose that lending institutions be required to disclose 1) how many identity theft incidences they suffered or avoided, 2) the form of identity theft attempted (i.e. new account fraud, credit card fraud, etc.) and the product targeted (mortgage loan, credit card, etc), and 3) the amount of loss suffered or avoided.

If lending institutions reported limited information about identity theft, I believe it would reveal that identity theft is both more prevalent and economically damaging than currently acknowledged, in part because of the rise of "synthetic identity theft," a form that cannot be measured by victim surveys because they are unaware of the crime. Furthermore, the disclosure requirement would birth an anti-identity theft market, and the prevalence and severity of the crime would decrease dramatically as institutions compete to offer the safest financial products to consumers.

## **Conclusion**

We believe that many cases of identity theft could be stopped at their inception if lending institutions simply used tools already available to them. The rise of synthetic identity theft demonstrates that some lending institutions are not authenticating the identities of credit applicants. Other examples of negligent credit granting further point to the need to change practices and procedures in order to curb identity theft. On a more fundamental level, we need better data on identity theft to learn about trends, and to tailor responses to the crime.

Thank you for considering our request to participate in the Workshop to discuss these issues.

---

<sup>20</sup> One of ITRC's clients had over \$7,000,000 in fraud using his identity. IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003 27-28 (Sept. 23, 2003), available at <http://www.idtheftcenter.org/idaftermath.pdf>.

Respectfully submitted,

/s

Chris Hoofnagle  
Senior Staff Attorney  
(510) 643-0213