

ELECTRONIC PRIVACY INFORMATION CENTER

Before the Federal Trade Commission

Comments of the Electronic Privacy Information Center
on the ID Theft Survey: FTC File No. P034303

The Electronic Privacy information Center (EPIC) appreciates the Commission's efforts in researching and combating identity theft, and submits these comments for further improvement of the Commission's survey studying the incidence and prevalence of identity theft in the United States. EPIC is a non-profit public interest research organization founded in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, free speech, and constitutional values. EPIC has been involved in identity theft policymaking for several years, testifying before Congress and submitting comments to the Commission on identity theft issues.

The Commission's survey work to date has given the public insight into the problems of identity theft in the United States. The polling of 5,000 individuals indicated the scale of identity thefts in America (an estimated 10 million), as well as the considerable expense and time that victims lose to identity theft (5 billion dollars and 397 million hours in the past year, respectively).¹

However, EPIC proposes certain improvements in the new survey. Specifically, an increased sample size and data from credit grantors could further help the Commission in its efforts against identity theft. A larger sample size than the 5,000 individuals polled

¹ Federal Trade Commission, Identity Theft Survey Report 28, Sept. 2003, *available at* <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>.

in the 2003 survey would give a more accurate picture of the scope of the problem, and consumers' ability to deal with the repercussions.

Furthermore, what is often missing from discussions on identity theft, however, is consistent information from businesses, particularly credit grantors, on practices that may contribute to the risk of identity theft. EPIC recommends that the Commission poll credit grantors in three particular areas: (1) the use of authentication standards, if any, before granting a new tradeline, (2) the number of granted and refused credit applications, and (3) the number of applications that result in fraud.

All of these questions would help assess the grantors' measures to ensure that fraudulent applicants are not granted new credit accounts. In addition, this information would provide a useful follow-up to the findings of the Federal Deposit Insurance Corporation's 2004 study on identity theft, which specifically recommended the use of two-factor authentication for customer authentication systems.

There is a growing body of evidence that suggests that creditors do not adequately screen credit applicants before issuing tradelines.² 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. For instance, in *Nelski v. Pelland*, 2004 U.S. App. LEXIS 663 (6th Cir. 2004), a phone company issued credit to an impostor using the victim's name but a 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 Number of employees-victims but directed all six to be sent to the impostors' home. In *Aylward v. Fleet Bank*, 122 F.3d

² See, e.g., Adam Smith, *Ruining my credit was easy, thief says*, St. Petersburg Times, Oct. 23, 2005, available at http://www.sptimes.com/2005/10/23/Worldandnation/Ruining_my_credit_was.shtml.

616 (8th Cir. 1997), the bank issued two credit cards based on matching name and Social Security Number but 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. 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.

In light of these cases, where individuals included glaring errors in the application and still obtained credit, identity theft expert Beth Givens has argued that many incidences of the crime could be prevented by simply requiring grantors to more carefully review credit applications for obviously incorrect personal information.³ Survey questions on these practices will help determine the extent to which creditors themselves are responsible for identity theft.

Questions on credit grantors' practices will also maintain focus on correcting flawed policies and practices, instead of shifting the blame to consumer behavior. Many in the data industry have misrepresented findings in the Commission's report to "blame the victim" in identity theft cases. For instance, Fred Cate has testified before Congress that "The FTC's September 2003, study on identity theft indicated that 76 percent of identity theft cases involved a friend, family member, coworker, neighbor or an employee of somebody who has lawful access to the SSN. Restricting the further transmission or the display of the SSN would not be relevant in those cases, the vast majority of cases."⁴

³ *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).

⁴ Hearing on Enhancing Social Security Number Privacy, Before the House Ways and Means Subcommittee on Social Security (testimony of Fred Cate, Professor of Law, University of Indiana-Bloomington), Jun. 15, 2004, available at <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=1647>.

However, Mr. Cate's 76 percent figure is not based on all identity theft victims. Instead, it is based on a selective minority of identity theft victims—those few who knew the actual identity of the impostor ("in 26% of all cases, the victim knew who had misused their personal information").⁵ We urge the Commission to clearly explain its findings so that misinterpretations can be reduced.

Finally, information about identity theft at its inception, rather than only after its discovery by consumers, would add valuable insight into the growing problem of identity theft. EPIC again appreciates the Commission's work in this matter and the opportunity to comment on this valuable project.

Chris Hoofnagle
Director, EPIC West
944 Market St, Suite 709
San Francisco, CA
94102

Sherwin Siy
IPIOP Staff Counsel
EPIC
1718 Connecticut Ave NW, Suite 200
Washington, DC 20009

⁵ Federal Trade Commission, Identity Theft Survey Report 28, Sept. 2003, *available at* <http://www.ftc.gov/os/2003/09/synovatereport.pdf>.