WORLD **PRIVACY** FORUM

Via Electronic Submission to https://secure.commentworks.com/FTC-IDTSurvey

December 19, 2005

Federal Trade Commission
Office of the Secretary,
Room H-135 (Annex E)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: ID Theft Survey: FTC File No. P034303. [Federal Register 18 November 2005, 69970, Vol. 70, No. 222].

Pursuant to the notice published in the Federal Register on November 18, 2005 regarding the Federal Trade Commission's proposed identity theft survey, the World Privacy Forum respectfully submits the following comments.

The World Privacy Forum is a non-profit, non-partisan public interest research organization. It focuses on in-depth research and analysis of technologies and their impacts, with a particular view to the privacy and security implications of emerging and maturing technologies and data infrastructures.

The Federal Trade Commission is thoughtfully re-examining its 2003 identity theft survey instrument and has requested public comments on this matter. We appreciate the opportunity to comment on the proposed survey; following are our comments on this issue.

Request for Analysis of Sample Size Prior to Conducting New Survey

We request that the FTC analyze its proposed sample size of 5,000 for the ID theft survey to bring it to the optimum level, whatever that level may be. Validity of sample sizes can vary with subject matter and other factors. For this reason, we cannot make a

firm recommendation on sample size without knowing more about the analytical methods the FTC plans to use in its proposed survey. However, we would like to point to the American Statistical Association's Ethical Guidelines for Statistical Practice, which states that entities should "Avoid the use of excessive or inadequate numbers of research subjects by making informed recommendations for study size. These recommendations may be based on prospective power analysis, the planned precision of the study endpoint(s), or other methods to assure appropriate scope to either frequentist or Bayesian approaches."[1]

The FTC survey on identity theft should be an authoritative survey; it is therefore important to have a sample size that is well-researched, well-supported, and not subject to procedural criticism.

Adding Questions on Impact of Security Breach Notice

We request that the FTC include questions in its survey instrument regarding security breach notifications. Specifically, we request that the FTC formulate questions that will acquire the following information:

1. If a consumer received a security breach notification.
2. If yes, then information about whether a consumer was a subsequent victim of identity theft in any form.
3. If yes, what if any specific steps a consumer took to reduce their risk of identity theft after the breach notification, for example, putting fraud alerts on accounts, freezing credit reports, and so forth.

Security breach notification is, relatively speaking, a new issue that has not been exhaustively and authoritatively studied to date by an entity without some financial stake in the outcome. The FTC survey is an excellent opportunity to shed light on how security breach notification interacts with the consumer experience of identity theft.

[1] American Statistical Association, Ethical Guidelines for Statistical Practices, < http://www.amstat.org/profession/index.cfm?fuseaction=ethicalstatistics >.

Some studies of security breach notification have noted that, for example, large security breaches do not typically result in identity theft. However, we wonder if the security breach notice has had its intended effect of protecting consumers by allowing them the opportunity to monitor credit and prevent problems from occurring. Because this is a new area of inquiry, because of its importance to the consumer, and because the states and Congress are actively pursuing legislation in this area, security breach notification should be added to the FTC's survey instrument.

Adding Questions on Definitional Understanding

We request that new questions are added to the survey instrument that clarify the respondents' baseline understanding of identity theft. It is our experience that consumers define identity theft in numerous and sometimes contradictory ways. Therefore, the final survey instrument needs to be fine-tuned to counter potential difficulties due to definitional issues. Two questions from the 2003 survey illustrate this challenge:

> 3. Did someone attempt to "TAKE OVER" the credit card account that had been misused by, for example, changing the billing address on the account or having themselves added as an authorized user of the account? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH.)
>
> 4. Have you ever been the victim of a different form of Identity Theft, one that involved more than just the misuse of existing accounts or numbers? That is, has anyone used your personal information without your permission, to obtain NEW credit cards or loans in your name, run up debts in your name, open other accounts, or otherwise commit theft, fraud, or some other crime? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE.)

These questions require some knowledge of the terms "take over" and "identity theft." We request that a definitional question is asked about the term identity theft prior to the first questions asking about the process of identity theft. We also request that if the term of art "takeover" or "account fraud" is used, that the terms are defined more clearly and to a greater degree of specificity, not just by an example that may or may not apply to the consumer.

Adding Questions to Clarify Medical Identity Theft

The World Privacy Forum is aware of the theft of consumer financial and insurance information in the practice of what we are calling "medical identity theft." In medical identity theft, consumers' information is used to gain medical treatment, services, and supplies. We request that the FTC add new questions to its survey instrument to find out more about identity theft in this specific area and what primary populations it is occurring in.

Recent examples of this problem include the following:

- July 26 2005, Pennsylvania Attorney General Tom Corbett announced an action against a 51 year-old Philadelphia man who used another individual's name and health insurance information to obtain medical care at five different hospitals in Philadelphia and in New Jersey. The medical identity thief raked in over $144,000 by repeatedly using this individual's name and medical insurance information without that person's knowledge or permission. The identity thief's hospital bills were submitted to Aetna Insurance, which paid $56,230 in claims before halting payments. [2]

- July 15 2005, a Lufkin, Texas identity theft victim received someone else's medical bills after that individual used the Texas man's identity to get medical treatment. The only tipoff the victim received about the problem was the bill after the fact.[3]

- In California, unscrupulous medical providers were buying Medi-Cal and Medicare patient identity numbers and were using them to get reimbursed for millions of dollars in tests and other services that were never provided. Of $34 billion annually spent by the Medi-Cal program for health care for approximately 7 million Californians, state officials estimate that as much as $14 billion of that amount is stolen in similar

[2] See < http://www.attorneygeneral.com/press/release.cfm? p=63807E79-F7D8-C5FB-113945CD4CCB12C7>.
[3] The Lufkin Daily News, 15 July 2005, Police Report.

fraudulent scenarios.[4] The California Medi-Cal identity theft scam specifically involved bad actors using stolen patient information purchased for as little as $100. During interrogations, investigators learned that workers in medical records offices and billing departments had copied the information for cash. Investigators said searches have turned up medical charts in the process of being altered.

Medical identity theft may be underreported. The unique aspect of medical identity theft is that it can potentially endanger consumers' lives due to the altering of medical files without consumers' knowledge. Altered medical files, for example, occurred in the California Med-Cal identity theft. It is therefore of key importance to understand and to prevent this form of ID theft.

In the 2003 survey, question number 19 dealt specifically with medical identity theft. The question was as follows:

> 19. You indicated that one or more of your existing accounts other than credit card accounts had been misused. Of those accounts you already had did the person run up charges on, or otherwise misuse, any of the following accounts. Did the person misuse your ... (INSERT AND RANDOMIZE ACCOUNTS)? (DO NOT READ ANSWER LIST. ENTER SINGLE RESPONSE FOR EACH ACCOUNT.)
> Don't Yes No Know Refused
> Checking or Savings Accounts.....1 2 X R
> Insurance Accounts, including Medical, Auto, and Life.....1 2 X R
> Internet or E-Mail Accounts.....1 2 X R

This question does not lead to a separate, refined response about medical identity theft. We request that medical identity theft is asked in a separate question and not pooled into a generalized insurance question including auto and life policies.

Anecdotal information hints that most people do not know about medical identity theft until they receive a bill for services or find errors in their medical charts. It would be a step forward to be able to get substantiation as to whether or not this is correct through adding a new question or questions that would request this information. It would also be extremely helpful to hear from consumers how long/how many hours it took for them to

[4] See "Medi-Cal Fraud Flourishing on Black Market," Jason Kandel, 7 August 2005, Los Angeles Daily News.

correct problems arising from medical identity theft, and what kind of redress they received. For example, did the insurance company simply pay for all costs, and the consumer had little to do to correct the problem? What specifically was involved with resolving this form of identity theft?

Additionally, much of what happens in medical identity theft appears to be account takeover. However, there are no hard statistics on this, either. Any light the FTC survey could shed on this would be helpful.

Including Questions to Clarify "Account Fraud," Resulting Harm, and Form of Identity Theft Issues Across Sectors

A. Need for statistics highlighting correlation and overlap between forms of ID theft

Philosophical and definitional differences regarding the issue of "account fraud" versus "identity theft" exist, and these issues require substantial clarification. Some articulate identity theft in a broader way than others. The differences in these baseline understandings of what identity theft is and the harm it causes to consumers have led to criticism of survey instruments that do not align with one philosophical side or the other.

The issue of "account fraud" is contentious and has not been resolved in part because of definitional issues, but also because there is not a clear set of statistics that have been set forth by a neutral party to substantiate the intersecting aspects of this matter to a high degree of trust. For example, there is not a clear set of numbers that delineate what percentage of consumers with "account fraud" in various sectors (financial, medical, etc.) *also* experience other forms of identity theft. It is entirely possible that in a high percentage of cases, "account fraud" occurs contemporaneously with identity theft.

The FTC addressed the definitional issue of account fraud in part in its work on "Forms of ID Theft" in the 2003 survey. Questions 1, 19, and 20 dealt with existing accounts, and questions 24, 25, and 27 dealt with new accounts. But there was not a set of questions that showed the precise correlation and overlap between the two. For example, if one was looking at a Venn diagram of the two forms of ID theft, how large is the

portion of overlap between the two forms of ID theft? We do not know the answer to this question. We request that the FTC include consumer questions that will provide answers to the question of correlation and overlap in the area of forms of ID theft.

B. Clarifying sectoral differences regarding account fraud: Medical vs. financial

We do not have definitive answers to questions about consumer harm resulting from different forms of identity theft across sectors, which anecdotal information suggests can vary widely.

The financial services industry has largely argued that "account fraud" is not the same as identity theft, and that it does not harm consumers substantially due to the protections offered by the financial services industry. For example, Visa, in its October, 2005 comments to the FTC on the ID theft survey stated that "The risk of consumer harm from account fraud is significantly different than the risk of harm from identity theft."[5]

"Account fraud" is often defined as the misuse of an existing account. As already mentioned, in the financial services industry, its claim is that account fraud does not lead to great consumer harm. (Consumers may have an entirely different opinion of this claim.) In instances of medical identity theft, "account fraud" can potentially lead to extraordinary harm due to misinformation that may be added to a medical file. "Account fraud" in this context, therefore, may involve significantly different kinds of numbers and harm than in a credit card context.

Given that consumers may suffer potentially significant harm from "account fraud" in some contexts, does the definition of account fraud change across contexts, or does it remain the same? This question has not been answered yet. If the FTC survey can gather some clear statistical data in this area, it will be an important step toward clarifying these issues.

To sum up, in setting up the consumer questions in this area, we encourage the FTC to consider harm from "account fraud" in areas other than just credit card services, for example, medical.

---

[5] Public comments by VISA on the FTC Identity Theft Survey, October 24, 2005. See <http://www.ftc.gov/os/comments/idtheftsurvey/index.htm>.

C. Industry information can help clarify definitional and correlation challenges

In order to begin to get some hard numbers on this issue and begin to understand it, it will be important for the FTC to also acquire statistical information from the financial services industry. We understand and acknowledge that this is a consumer survey. However, we also acknowledge that information from credit grantors and insurors can provide a crucial piece of the puzzle in this area and enhance our understanding of the mechanisms of identity theft in its various forms.

We request that the FTC ask questions that acquire the following information from financial service companies:

1. How much "account fraud" has occurred over specific periods of time, for example, the year 2004 or 2005, or both?
2. What are the specific losses due to account fraud during the specified period?
3. How many consumers make/have made fraud-related requests to credit grantors during this period? For example, accounts flagged, cards replaced, and so on.
4. How many instances of fraud related to account takeover and other forms of ID theft have insurance and financial companies documented? What are the losses in this area?
5. If credit grantors have evidence that consumers with account fraud are not *also* identity theft victims, this information should be shared with the FTC.
6. Definitional: How does the financial service industry define account fraud? How does the financial service industry define account takeover? How does the financial service industry define identity theft?

A second cluster of important issues that industry could help clarify surrounds how credit is granted to consumers, and how often. We request that the FTC ask credit grantors to clarify the following issues as part of the survey process:

1. Authentication practices:

- How many identifiers does the financial institution require before granting credit? (For example, is the institution using two-factor authentication?)

2. Application process:
   - How many pre-screened applications are refused over what period of time?
   - What percentage of pre-screened credit applications result in fraud for the same period as above?
   - What total percentage of credit applications result in fraud?

To summarize, we request that the FTC include questions that clarify:

- The correlations that exist specifically between forms of ID theft such as "account fraud" and other forms.
- The consumer experience of harm in account fraud across multiple sectors (financial, medical, other as appropriate).
- Industry numbers and statistics that will fill in gaps in understanding the complete picture relating to forms of ID theft.

Getting More Information About Lack of Reporting of ID Theft

One of the more intriguing results of the 2003 survey was contained in consumers' responses to questions number 33, 33a, 36, and 41 about reporting ID theft. The 2003 survey found that "Only about 25 percent of victims who participated in the survey said that they had reported the crime to local police. Even with the more serious "New Accounts and Other Frauds" form of ID Theft, only 43 percent of victims said that they had reported their experiences to local police." Further, the 2003 survey found that "Only 22 percent of ID Theft victims said that they had notified one or more credit bureaus about their experiences."

These findings are significant, and we would like to understand the underlying causal mechanisms driving this phenomenon. For this reason, we request that the FTC include a follow-up question or questions that ask consumers who did not report their experience(s) of identity theft why they did not report it.

*****

The FTC consumer identity theft survey holds an important role in the debate, study, and efforts toward prevention of identity theft. For this reason, the survey needs to be thorough in its approach and needs to rest on an appropriate statistical sample size.

We appreciate the FTC's important work in this area. We believe that by adding questions on security breach, medical ID theft, by clarifying forms of ID theft, and by asking for statistical information from the financial industry, that the next survey will be of great help in aiding all stakeholders, including consumers, the financial community, and law enforcement.

Respectfully submitted,

Pam Dixon
Executive Director
World Privacy Forum
www.worldprivacyforum.org
+1 760.436.2489