Federal Trade Commission
Identity Theft Prevention Workshop

COMMENTS OF THE NATIONAL RETAIL FEDERATION

The National Retail Federation (NRF) welcomes the opportunity to contribute these comments to the Federal Trade Commission forthcoming Identity Theft Prevention Workshop. As the world's largest retail trade association, NRF's mission is to conduct programs and services in research, education, training, information technology, and government affairs to protect and advance the interests of the retail industry. NRF's membership includes the leading department, specialty, independent, discount, and mass merchandise stores in the United States and 50 nations around the world. NRF represents more than 100 state, national, and international trade organizations, which have members in most lines of retailing. NRF also includes in its membership key suppliers of goods and services to the retail industry.

The NRF wishes to highlight four features of identity theft, its causes and impact, and the fundamental tension that exists between efforts to prevent identity theft and other valuable uses of personal information, and then to provide seven specific recommendations for how the government might help prevent identity theft and track down identity thieves.

1. The Identity Theft Conundrum

"Identity theft" presents lawmakers, consumers, and businesses with an inherent conundrum: The very attributes of modern commerce that consumers value and expect—rapid, easy, 24-hour access to a wide variety of innovative products, services, and information—make identity theft easy to perpetrate and difficult to detect. Similarly, the most effective tools for preventing and detecting identity theft often interfere with that speed and convenience.

This conundrum is exacerbated when identity theft is categorized as a "privacy" issue or used to justify additional privacy laws. In reality, identity theft is often greatly facilitated by privacy, and the most effective tools for addressing identity theft involve the disclosure and use of additional personal information.

For example, how does a merchant verify that a customer presenting a check or credit card or requesting instant credit is in fact who he claims he is? The only way is to require that the customer provide *more* information or *more* forms of identification. Yet few customers are willing to tolerate being asked for a second or third piece of identification when making a simple purchase (privacy advocate Beth Givens testified before Congress in July 2000 that federal law should *require* credit grantors to verify at least *four* pieces of information[1]), and few consumers would consider a service convenient or rapid (much less "instant") if we were required to carry a

[1] Identity Theft: How to Protect and Restore Your Good Name, Hearings before the Subcomm. on Technology, Terrorism and Government Information of the Comm. on the Judiciary, U.S. Senate, July 12, 2000 (statement of Beth Givens, Director of the Privacy Rights Clearinghouse).

passport or birth certificate to avail ourselves of it. Moreover, these and other forms of government-issued identification are often fraudulent themselves; indeed, according to one 2000 survey of identity theft victims, 45 percent of their cases involved fraudulent drivers' licenses.[2]

The Internet only exacerbates these concerns. How does a Web merchant verify the identity of a customer using a credit or debit card or applying for instant credit? There is at present no way to "see" photo identification over the Web, so most retailers today deal with this problem by asking for *more* information. Privacy advocates argue that soliciting this additional information violates privacy and bills are pending that would prohibit the use of Social Security Numbers for this purpose, yet the failure to obtain and verify this information leaves the field wide open for identity thieves.

As these examples illustrate, privacy protections, rather than being logically motivated by concerns about identity theft, are often wholly at odds with efforts to prevent identity theft. And this in turn is the result of the fundamental conundrum that identity theft is largely the result of the speed, convenience, ubiquity, and in many cases, anonymity that characterize modern information flows and that are essential to the ready access to services, products, and information that consumers demand. Efforts to restrict that flow of information are unlikely to have much impact on identity theft, but they are certain create tremendous impediments to customer service and convenience.

2. The Financial Loss of Identity Theft-Related Fraud is Paid for by U.S. Businesses

Identity theft has many victims. The most obvious and personally affected are the individuals whose identity is stolen, who, in the words of a recent General Accounting Office report, "suffer from injuries to their reputations and must undergo a sometimes very lengthy and agonizing process of clearing up their credit history."[3]

However, one harm that identity theft victims do *not* suffer is having to pay for the fraudulent charges that identity thieves rack up in their victims' names. Under the Fair Credit Billing Act,[4] the Electronic Funds Transfer Act,[5] state laws,[6] and company policies, those charges are virtually always paid by the merchants from which the goods or services were fraudulently obtained, or the financial institutions who extended credit or whose charge or debit cards were fraudulently used by the identity thieves.[7]

---

[2] CALPIRG and Privacy Rights Clearinghouse, Nowhere to Turn: Victims Speak Out on Identity Theft 3 (2000).

[3] General Accounting Office, Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (1998).

[4] 15 U.S.C. §§ 1601 et seq.

[5] 15 U.S.C. §§ 1693 et seq.

[6] A Crook Has Drained Your Account. Who Pays?, FDIC Consumer News, Spring 1998, available at http://www.fdic.gov/consumers/consumer/news/cnsprg98/crook.html.

[7] Federal Trade Commission, ID Theft: When Bad Things Happen to Your Good Name 17 (2000);

More than 1.2 million worthless checks are cashed at retailers, banks, and other U.S. businesses every day, accounting for $12.6 billion in losses. Credit card issuers lost $668 million in 1998 due to fraudulent charges, and the Treasury Department officials estimate total credit card fraud losses to be between $2 billion and $3 billion in 2000.[8] The insurance industry paid $20 billion in 1999 for fraudulent property and casualty claims. Across the economy, business losses due to all forms of document fraud and counterfeiting exceed $400 billion—6 percent of annual revenue—per year.[9] These losses affect the businesses that must absorb them, as well as consumers through higher prices, inconvenience, and lost time and productivity. The government should therefore be careful to avoid increasing the cost of identity theft and related frauds to U.S. businesses.

3. Some Government Agencies Have Unwittingly Contributed to Identity Theft.

Until quite recently, many government agencies have done more to facilitate identity theft than to prevent or remedy it. For example, the government, motivated by a laudable desire to serve citizens, has made it easier than ever to obtain identification documents. Identity thieves take advantage of that new ease and use it to obtain fraudulent identification documents, such as drivers licenses and birth certificates. These, then, are the keys to unlocking an individual's financial record.

Similarly, the government's inability or unwillingness to correct judicial and law enforcement records has contributed significantly to the harm experienced by victims of identity theft when they are arrested—often repeatedly—for crimes they did not commit, or they are denied benefits because of bankruptcies they did not file.

Virtually all victims of identity theft report that the injury they suffer is greatly exacerbated by the difficulty of working with the police and other government agencies to repair their credit and reputations, and apprehend the perpetrators. One identity theft victim, typical of the stories of many others, told the authors of a recent survey on identity theft: "The police department treated me as if I were the criminal."[10] According to the authors of the survey, "[v]ictims reported the same difficulties with other government agencies they dealt with. Many responded that the Postal Inspector and the Department of Motor Vehicles told them nothing could be done, even if the theft had involved the victim's mailbox or driver's license."[11] This is the near-universal refrain from identity theft victims:

> It is aggravating, debilitating and depressing beyond belief to meet with this kind of response at virtually every place one calls to get some assistance. One is advised to follow the proper channels, but the proper channels yield impotence at

---

[8] Gary Fields, Victims of Identity Theft Often Unaware They've Been Stung, USA Today, March 15, 2000, at 6A (quoting Undersecretary James Johnson of the U.S. Treasury Department).

[9] Association of Certified Fraud Examiners, Report to the Nation on Occupational Fraud and Abuse, available at http://www.cfenet.com/newsandfacts/fraudfacts/reporttothenation/reportsection4.shtml.

[10] Nowhere to Turn, supra at 6.

[11] Id. at 7.

best, hostility toward the 'annoying' victim at worst. They are more like obstacles to tangible assistance.[12]

One of the major issues concerning identity theft today is how to accurately separate data about one individual from data about another. This is made all the more difficult by the fact that approximately 16 percent of the U.S. population—about 42 million Americans—changes addresses every year; there are approximately 2.4 million marriages and 1.2 million divorces every years, often resulting not only in changed addresses, but also changed last names; and, as of 1998, there were 6 million vacation or second homes in the United States, many of which were used as temporary or second addresses.[13]

The only reliable way to date to ensure that information about one consumer is not erroneously provided to another consumer or added to another consumer's file is to organize those files by SSN. Yet Congress is presently considering a number of bills that would restrict the use and disclosure of SSNs. Proponents of such legislation argue that such legislation is necessary to limit the availability of SSNs in the market and thereby reduce their availability for use in identity theft.

This ignores the fact that many cases of identity theft involve someone the victim knew—a relative, friend, or business associate.[14] The Chief Credit Office of Household International, Inc., testified before Congress in 1999 that half of all incidents of identity theft are committed by a *family member*.[15] Robert Hartle, one of the most well-publicized victims of identity theft and now a leading victim's rights advocate, discovered that his personal information had been taken by the estranged husband of his mother.[16]

Moreover, it is questionable whether legislation restricting the responsible use of SSNs by business will have an appreciable effect on diminishing their availability for identity theft if every personnel record, payment, and interest-bearing or dividend-paying account still required a SSN. But it is certain that such a law would greatly increase the likelihood of identity theft and innocent errors by making it harder to identify specifically a unique individual. Retailers' use of SSNs, rather than being a significant source of information for identity thieves, is often a significant protection against identity theft. This highlights the irony that identity theft is largely the result of the speed, convenience, ubiquity, and in many cases, anonymity that consumers value, and that many current and proposed privacy protections are often wholly at odds with efforts to prevent identity theft.

---

[12]Id.

[13] Use and Misuse of Social Security Numbers, Hearings before the Subcomm. on Social Security of the Comm. on Ways and Means, U.S. House of Representatives, 106th Cong., 2d Sess., May 11, 2000 (statement of Stuart K. Pratt, Vice President, Government Relations, Associated Credit Bureaus, Inc.).

[14] Nowhere to Turn, supra at 3.

[15] Identity Theft, Hearings before the Subcomm. on Telecommunications, Trade & Consumer Protection and the Subcomm. on Finance and Hazardous Materials of the Committee on Commerce, U.S. House of Representatives, 106th Cong., 1st Sess., April 22, 1999 (statement of Charles A. Albright, Chief Credit Officer, Household International, Inc.).

[16] Michael Higgins, Identity Thieves, ABA Journal, Oct.. 1998.

Solutions

There are better solutions that recognize the inherent tension between protecting consumer benefits, including privacy, on the one hand, and preventing identity theft on the other. These solutions seek to balance competing interests to provide the maximum benefits with least risk to consumers.

Retailers are already actively implementing many new programs designed to make identity theft more difficult. They have enormous incentive to do so because they, along with other businesses, bear virtually all of the growing financial cost of fraud associated with identity theft. Many retailers are expanding their efforts to develop and employ better methods for authenticating the identity of consumers who open accounts, apply for instant credit and credit and debit cards, and seek to change basic information about an account. This requires, in appropriate contexts, the use of biometric identifiers (such as fingerprints). In addition, many retailers are expanding their account monitoring to detect fraud. Account monitoring has proven to be one of the most effective methods for identifying fraudulent transactions and victims of identity theft, especially when that monitoring occurs across accounts and across affiliates, so that the merchant has more comprehensive and precise knowledge of transaction patterns. A number of pending privacy laws threaten to restrict the ability of retailers to use this identity theft detection strategy or to condition account monitoring on consumer consent.

One of the most important role in the fight against identity theft, however, is played by the government, because the government provides the identification tools that business and consumers rely on, the government enforces the laws against identity theft and related frauds, and the government establishes the laws that facilitate or restrict the tools that business and consumers rely on to prevent identity theft. There are at least seven important tasks that the government—both federal and state—should undertake:

1. The government should make government-issued forms for identification harder to obtain. Driver's licenses, state identification cards, birth certificates, passports, Social Security cards, military identification—these are the tools that the rest of the economy relies on to verify identity. If they are easily forged or fraudulently obtained or "taken over," then their value in the economy diminishes greatly, and the government actively disserves consumers and businesses alike. Today, a large percentage—perhaps a majority—of frauds committed by identity thieves involve obtaining new government-issued identification. The government must stop being the unwitting accomplice of identity thieves.

2. The government should make the promise of centralized reporting of identity thefts a reality. A single database should link all law enforcement agencies so that a victim can make a report to his or her local police department and have that information instantly be available to other law enforcement agencies across the country. Moreover, the government should establish a parallel or linked database to which anyone with a legitimate interest and appropriate consent of the individual involved can have access to verify that an incident of identity theft has been reported. This would create a national

"fraud alert" system that would help prevent any additional use of stolen identities, facilitate the identification of identity thieves, and provide victims of identity theft with a single source to which they can direct creditors, employers, and others to verify claims of identity theft. This aids consumers directly, by helping them clear their names, but it also helps them indirectly, by allowing merchants to rapidly identify and assist consumers with legitimate identity theft claims, while also detecting the as many as 60 percent of claims that are erroneous or fraudulent.[17]

3. The government should make it easier to correct judicial and criminal records, to remove permanently from one individual's record references to acts committed by an identity thief. No one other than the government can perform this vital task, and the incidents of victims of identity theft being arrested—in some cases repeatedly, denied jobs, and even detained at the border all for crimes committed by another in their names illustrates the urgency of speedy action.

4. The government needs to improve enforcement of identity theft and related crimes. Clearly, there have been significant improvements following passage of the Identity Theft Assumption and Deterrence Act, but enforcement requires financial and personnel resources that only the legislative branch can authorize. More innovative, well-funded approaches are necessary to apprehend and convict identity thieves and to help victims clear their credit records and good names.

5. The government should help educate consumers about the practical steps that they—and often only they—can take to prevent identity theft. For example, consumers should closely monitor their accounts for unusual or unexplained transaction or for missing statements or replacement credit cards. Early knowledge is one of the best ways of restricting the thief's use of stolen personal information. Of course, early knowledge is only useful if the consumer reports the fact to creditors, credit bureaus, and law enforcement authorities. And many consumers are our own worst enemies when it comes to preventing identity theft, because of the cavalier way in which we select and use account names and passwords, disclose personal information to strangers, and fail to protect our credit cards and checks. Nothing can substitute for good judgment in the management of our personal information and identification document for its effectiveness in combating identity theft.

6. Not all of the government's obligations with regard to identity theft require action: The government must also refrain from well-intentioned actions that have the unintended effect of limiting the tools that consumers and businesses use to fight identity theft. This is especially true given that the variety of recently enacted laws applicable to identity theft and the fact that the major new federal law—the Identity Theft Assumption and Deterrence Act—was only enacted in late 1998. Moreover, the government should avoid

[17] Alternative Dispute Resolution for Consumer Transactions in the Borderless Online Marketplace, U.S. Federal Trade Commission and Department of Commerce, June 6, 2000, at 148 (statement of Russell Schrader, Senior Vice President and Assistant General Counsel, Visa USA); Identity Theft, supra (statement of Charles A. Albright, Chief Credit Officer, Household International, Inc.).

enacting laws that restrict the availability and responsible use of critical information that helps businesses authenticate the identities of consumers, manage information about them accurately and responsibly, and protect it from unauthorized access or use. Laws prohibiting the use of SSNs for identifying and separating consumer information, that limit the use of fingerprints and other biometric identifiers, or that restrict the ability of retailers to verify the accuracy of consumer information with affiliates and third parties greatly diminish the ability of businesses to protect consumers from identity theft.

7. Lawmakers should explicitly acknowledge the frequent tension between identity theft and privacy and the trade-offs between preventing and detecting identity theft and providing the services that consumers expect and demand. The government should be careful to balance any measure designed to protect against identity theft with the other costs it imposes on consumers and businesses.

Conclusion

Many important initiatives are already underway to help stem the tide of identity theft. But the success of these strategies depends in large part on the government making it harder for identity thieves to obtain fraudulent identification documents, easier for victims of identity theft to report the crime and clear their names, and more likely that identity thieves will be caught, prosecuted, and jailed.

It is equally important, however, that the government avoid taking the wrong steps. Identity theft presents a real conundrum, because it is the same rapid, easy, 24-hour access to products, services, and information that consumers value that make identity theft easy to perpetrate and difficult to detect. And the most effective tools for preventing and detecting identity theft often interfere with that speed and convenience. The government must therefore be careful to avoid imposing overly burdensome restraints on the responsible use of personal information; they may make identity theft more difficult, but they will also make beneficial services impossible, impractical, or unduly expensive.

The identity theft conundrum is only exacerbated when identity theft is categorized as a "privacy" issue or used to justify additional privacy laws. In reality, identity theft is often greatly facilitated by privacy, and the most effective tools for addressing identity theft involve the disclosure and use of additional personal information. The government should therefore avoid enacting laws and regulations that interfere with the tools and diminish the power of consumers and businesses to fight identity theft.