



January 19, 2007

**Identity Theft Task Force (P065410)**  
Federal Trade Commission/Office of the Secretary  
Room H-135 (Annex N)  
600 Pennsylvania Avenue, N.W.,  
Washington, D.C. 20580.

Via e-mail to: [Taskforcecomments@idtheft.gov](mailto:Taskforcecomments@idtheft.gov).

Ladies and Gentlemen:

The Identity Theft Assistance Corporation (the “Corporation”) appreciates the opportunity to provide the Federal Identity Theft Task Force with input on specific issues identified by the Task Force and several other critical issues relating to identity theft and the security of sensitive personal information.

Three years ago, under the leadership of The Financial Services Roundtable and BITS, fifty of the nation’s largest financial institutions came together to address the needs of identity theft victims, industry and law enforcement. The fifty founding members created the Corporation as a nonprofit membership corporation and provided the funding to launch the Identity Theft Assistance Center (“ITAC”), an innovative, collaborative industry initiative that helps victims of identity theft restore their financial identity, partners with law enforcement to catch and convict the criminals and helps the industry fight fraud.<sup>1</sup> ITAC leverages its experience in victim assistance and data breach management to support the industry’s continually improve fraud fighters. For convenience, the Corporation and ITAC are hereinafter referred to collectively as “ITAC”.

As the leader in helping victims and partnering with industry and law enforcement to fight identity theft, ITAC is uniquely equipped to assist the Task Force. Since its creation in 2004, ITAC has:

- Helped more than 11,000 victims restore their financial identity.
- Delivered nearly 20,000 fraud warnings to member and nonmember companies.

---

<sup>1</sup> A list of ITAC’s members is attached. For more information, please see our website at [www.identitytheftassistance.org](http://www.identitytheftassistance.org).

- Shared demographic and incident-related information relating to more than 11,000 verified cases of identity theft under landmark agreements with Federal Trade Commission, US Postal Inspection Service and the Regional Identity Theft Task Force in Philadelphia.
- Surveyed actual victims to determine the causes of identity theft.
- Partnered with leading academics on identity theft research.
- Distributed the Federal Trade Commission's identity theft consumer education package "Deter, Detect, Defend" to ITAC member companies.
- Been named by the UK's National Consumer Council as the model for victim assistance and public / private partnership for the UK.

### **ITAC's Victim Assistance Service**

Fortunately, true identity theft—the fraudulent opening of new accounts in the name of a consumer or the takeover of the consumer's existing accounts—is relatively rare, but its impact on victims and on society should not be underestimated. Identity theft is a vicious crime that terrifies its victims, robbing them of their time and peace of mind, as well as their money. Thanks to federal and state consumer protection laws, as well as initiatives by the financial services industry itself, consumers typically are not responsible for the money stolen by the identity thief; rather, the financial services industry incurs these losses. But consumers suffer the emotional consequences of the crime, and some have spent years restoring their credit and identity.

One of the principal difficulties that an identity theft victim encounters is the need to deal with multiple financial institutions and other companies, including retailers and utilities, with which the consumer may have had no previous contact.

Through ITAC's victim assistance service, which is provided free to customers of member companies, consumers can obtain the help and peace of mind they need at this difficult time. In addition, ITAC assists law enforcement by sharing information about verified cases of identity theft via the FTC's Consumer Sentinel database.

Consumers are referred to ITAC by a member company. In many cases, it is the member company that detects suspicious activity and contacts the consumer. In other cases, the consumer notices something—funds missing from an account or a collection call from an unknown company—and contacts the ITAC member.

First, the customer works with the ITAC member to resolve any issues at that company. The member gathers information about the event using the ITAC Uniform Affidavit. The ITAC disclosure explains that this information will be shared with other companies and with law enforcement. The sharing of information reduces the

burden on the victim who otherwise would have to tell his or her story repeatedly and complete multiple forms.

If the member determines that the problem involves identity theft, it offers the consumer the opportunity to use the ITAC service free of charge. The consumer typically is “warm transferred” to ITAC where, with the consumer’s consent, ITAC obtains the victim’s credit report. The ITAC agent reviews the credit report with the victim to see if there is evidence of accounts that have been taken over or fraudulent accounts that have been created. If the victim identifies suspicious accounts or inquiries (as 60% of consumers served by ITAC do), ITAC notifies the affected creditors. ITAC also places a fraud alert with the consumer reporting agencies if the victim has not already done so.

Each week, ITAC sends information about these cases to the United States Postal Inspection Service and the Federal Trade Commission to assist federal, state and local law enforcement investigations and prosecutions of identity theft crimes.

\* \* \*

Below are comments relating to ITAC’s experience followed by comments on the specific issues raised by the Task Force. For more information, we refer the Task Force to the letter from The Financial Services Roundtable and BITS.

### **ITAC’s Comments**

First and foremost, ITAC urges the Task Force to base its strategic plan on a partnership between the public and private sectors. The questions posed by the Task Force reveal an underlying assumption that the private sector and the public sector are separate worlds that can and should be subject to different expectations and requirements with respect to the use and protection of sensitive personal information. In fact, government agencies and private sector organizations interact so frequently and on so many levels – taxation, health care, employment and law enforcement to name just a few – that distinctions between the public and private sector on the use and protection of sensitive personal information are meaningless.

Moreover, the American public has the same high expectations of government agencies as it does of private sector companies. The reaction of consumers and lawmakers to data security breaches at the Veterans Administration and other governmental units, including the Department of the Navy, indicate that the public expects that when sensitive personal information is in the hands of a government agency, that information will be protected.

ITAC’s experience is that partnership works. When ITAC was first organized, some doubted that identity theft victims would agree to share information about themselves and the crimes with law enforcement. ITAC’s founding members believed that consumers’ thirst for justice would prevail and they have been proved

right. The unprecedented flow of data from ITAC to law enforcement agencies has been successful and shows great promise for the future. ITAC's law enforcement partners, including Lee Heath, the Chief Postal Inspector, and Patrick Meehan, the US Attorney in Philadelphia, report that ITAC data has helped their investigators and prosecutors find, investigate and convict suspects.

It is essential that the Task Force Report include an accurate and practical definition of identity theft as well as reliable and unbiased statistics on identity theft and fraud. Identity theft is the use of sensitive personal information to establish fraudulently new lines credit or open new accounts. Identity theft should be confused with simple fraud, such as the unauthorized use of a credit card. The aggravated abuse of an account which is often referred to as an account take-over is identity theft.

Equating every instance of fraud with identity theft is a disservice to the public and to policymakers. Exaggerated numbers create a climate of fear and helplessness which is not rooted in reality. Moreover, calling fraud identity theft is a disservice to consumers because the confusion about the nature and magnitude of the threat prevents consumers from effectively managing the real risks and from using the powerful remedial tools provided by the federal Fair Credit Billing Act, the Electronic Fund Transfer Act and similar state laws.

## **Issues Posed by the Task Force**

### **Maintaining Security of Consumer Data**

The financial services industry historically has met the challenge of maintaining the security of consumer data by means of reliable business controls as required by regulation, advanced technology, knowledge sharing, and cooperative efforts with government and law enforcement agencies. ITAC members view statutory data protection requirements as dynamic and work continuously to improve risk management systems and implement business practices to combat fraud and fight identity theft. Through organizations such as BITS, the financial services industry cooperates in analyzing threats, creating and adopting best practices, and partnering with the software and technology industries to provide more secure products and services.

The first two issues raised by the Task Force relate to the use of SSNs, specifically, exploring ways to reduce reliance on SSNs by federal, state and local government and surveying the use of SSNs by the private sector.

ITAC supports the Task Force's efforts to reduce the use of SSNs in the public sector. In recent years, financial institutions and other private sector entities have assessed the need to use SSNs in customer and employment relationships and have reduced the use of SSNs. Financial institutions also have adopted procedures, such

as truncation and technological tools including encryption, to protect SSNs when they are used. ITAC believes a similar effort by federal, state and local governments would enhance the protection of consumers.

With respect to a survey of the use of SSNs, as discussed above, ITAC supports the survey concept but believes that it must take a holistic approach and catalog the use of SSNs by the public sector as well as the private sector.

The Task Force also asked for input on whether it should recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. The recent compromise of sensitive personal information maintained by government agencies and by nonprofits, including universities and health care providers, demonstrate the importance of requiring all entities that maintain sensitive personal information, including federal, state, and local governmental units, and private sector entities including nonprofits, to safeguard such information.

A risk-based approach to securing sensitive personal information, as embodied in the Gramm-Leach-Bliley Act security requirements, has proved effective in the financial services industries and we believe would be successful in other industries, for nonprofits, and in the public sector.

With regard to notice, ITAC supports a national notification standard. Consistent with our comments above, we believe the standard should apply to public sector entities as well as private sector entities.

A uniform national standard will avoid serious implementation problems and inconsistent application. Efforts by various states and regulatory agencies create confusion for consumers and significant implementation problems for financial institutions. In a transient society, notification should occur uniformly regardless of where the consumer lives. Moreover, inconsistent application of inconsistent state law inevitably creates a compliance nightmare for institutions with a multi-state presence.

Notifying customers is a complicated and complex process and can, if poorly done, undermine confidence. Care must be exercised in alerting consumers to steps they can take to protect themselves from identity theft and fraud while averting needless alarm.

We support risk-based approaches for determining when and how to notify customers and to mandate notification only when there is some indication that the breach actually has the potential to cause harm or injury. If harm is demonstrably contained, for example, and no risk really exists, there should not be any reason to notify and scare people. ITAC supports requiring companies that discover data

security breaches to immediately notify law enforcement authorities, as well as consumer reporting agencies,

ITAC encourages the Task Force to support caps on damages. Any allowable damages should have firm caps and there should be no damages absent a showing of intent or actual harm. Absent negligence, an affirmative defense should be available if the company can demonstrate that it is a victim of fraud. We also support measures that provide “safe harbors” from lawsuits where reasonable notification procedures have been implemented and followed.

Education is an essential element of a national identity theft strategy and ITAC commends the Task Force for addressing this issue. However, the public sector should be an integral part of the educational campaign. Limiting the scope of an education campaign to consumers and the private sector would deprive governmental units and their employees and vendors of crucial information that they need to safeguard personal information in their possession.

Hands-on contact with thousands of identity theft victims provides ITAC and its member companies with deep understanding of how identity theft occurs and how this terrible crime affects its victims. In addition, ITAC has experience assisting companies in managing data security breaches. We look forward to sharing our experience with the Task Force and urge the Task Force to ensure that the educational efforts are fact-based. The failure to distinguish transactional fraud from identity theft and the use of inflated figures about the incidence of identity theft creates widespread fear and confusion and a feeling of vulnerability. We believe that the ITAC model of public / private partnership is working and that, going forward, a cooperative effort of government, industry and consumers can and will effectively manage the risk of identity theft.

### **Victim Recovery**

ITAC is a proven and successful model for helping victims of identity theft restore their financial identity. ITAC is actively seeking partners in other industries, including telecommunications, retailing and health care, and urges the Task Force to support growth of the ITAC model.

The Task Force invited comment on ways to make victims whole, including amending federal law to permit victims to seek restitution from the identity thief. In our view, restitution is likely to be time-consuming and frustrating for consumers and ultimately futile. Most identity theft victims do not experience out-of-pocket losses, non-financial damages are difficult to prove, and few identity thieves have the money to pay restitution.

The most serious harm that victims experience is non-monetary. It is the confusion, frustration and often extended delay in fixing the damage to the victim's life and reputation. Ways to help include:

- Police reports often are an essential first step for the consumer to establish that he or she is the victim and not the perpetrator. Government could help by making it easier for consumers to file police reports and easier for local police to accept reports of identity theft.
- Victims of identity theft report that they experience delay and inconvenience in dealing with government agencies including the Internal Revenue Service. The Task Force should explore ways to expedite a taxpayer's recovery process.
- Identity theft often affects aspects of a consumer's life that do not appear in a credit bureau report. Examples include drivers licenses and other forms of identification, medical care, and benefits including Social Security. The Task Force should explore ways to help victims find and correct these forms of identity theft damage.

Along those lines, ITAC supports further study of a national program to allow victims to obtain an identification document to prove their identity. It is important that any "passport" system can be used in the public and private sectors.

ITAC also supports research to assess the effectiveness of the FACT Act amendments and assessment of state credit freeze laws. Information about the costs and benefits of these laws will help policymakers evaluate the impact of these laws.

### **Law Enforcement**

ITAC supports the concept of a National Identity Theft Law Enforcement Center because, in our view, there are opportunities to improve the analysis of identity theft data available from ITAC and other public sector and private sector sources. We urge the Task Force to ensure that the new center does not duplicate or interfere with the work currently performed by the FTC.

ITAC also encourages the Task Force to find ways to increase state and federal prosecutions of identity theft crimes. In 2006, ITAC entered into a data sharing agreement with Regional Identity Theft Task Force in Philadelphia and applauds the success of the Philadelphia task force under the leadership of Patrick Meehan in coordinating the resources of local, state and federal law enforcement agencies.

As noted throughout this letter, the sharing of information between the public and private sectors is fundamental to the ITAC model. We support efforts to facilitate the exchange of information between the private sector and law enforcement agencies and encourage the Task Force to broaden the scope of its inquiry beyond financial services and include other business sectors including retailing, health care and telecommunications which possess information that can be vital to the investigation and prosecution of identity theft crime.

With respect to training, our experience suggests that the investigation and prosecution of identity theft crimes is limited by several factors. These include a lack of understanding on the part of investigators, prosecutors and judges of the human and economic costs of identity theft and a deficit in computer forensics training and experience. ITAC supports the efforts of the Alabama District Attorneys Association to create a National Computer Forensics Institute and the Task Force's interest in improving training generally for law enforcement with the suggestion that the Task Force include training for judges.

Finally, ITAC encourages the Task Force to actively pursue the gathering of additional data relating to identity theft including data relating to the human and economic costs of identity theft. We welcome the suggestion of adding questions relating to identity theft to the National Crime Victimization Survey which is great. Also urge the Task Force to learn more about the causes and costs of identity theft.

Thank you again for the opportunity to share our experience. If you have questions, please feel free to contact me at [anne@fsround.org](mailto:anne@fsround.org) or at 202.589.1936.

Very truly yours,

Anne Wallace