

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.
Taskforcecomments@idtheft.gov

Re: Comments on the Federal Identity Task Force

Dear Identity Theft Task Force members,

ING DIRECT appreciates the opportunity to comment on the Identity Theft Task Force Request for Public Comment which was released for comment on December 26, 2006. In this letter we provide the federal agencies that comprise the Task Force, the Federal Trade Commission, the Department of Justice and the interagency working group with comments and recommendations on those sections of the document which we believe we can provide the most useful input. This letter includes the exact text of the selected sections of the document followed by our comments.

ING DIRECT strongly believes that, while the federal agencies and the private sector have taken some action to address the growing epidemic of identity theft, more needs to be done. In that respect, we support the efforts of the Task Force and welcome the enhanced cooperation between government and the financial sector to protect the financial and private lives of consumers.

We as a financial institution, constantly strive to be proactive in preventing emerging risks to our customers and to our institution. Identity theft has been a primary area of focus for the past several years despite the introduction of continuously enhanced business controls and improved risk management systems.

One of the most important elements of setting a national strategy to prevent identity theft has to be the coordination of government and law enforcement efforts. The creation of a central agency to coordinate all efforts against identity theft and accumulate all relevant identity theft information should be the cornerstone of the strategy. Such an effort will improve measurement of the

instances of identity theft and economic impact while proving a data repository that can be used in a multitude of ways by the private sector.

I. MAINTAINING SECURITY OF CONSUMER DATA

1. *Government Use of SSNs*

Because SSNs are frequently used to facilitate identity theft, the Task Force currently is exploring ways to achieve reduced reliance on SSNs by federal, state, and local government. To the extent this is important, what steps (including working with state and local governments to highlight and discuss the vulnerabilities created by the use of SSNs and to explore ways to eliminate unnecessary use and display of SSNs) could help to achieve this goal? On a related issue, please provide any comments that you may have on what information could be used as a substitute for SSNs.

Comment:

ING DIRECT supports the reduced reliance on SSN by all government and private entities unless the need cannot be covered by another unique identifier, such as a username. However, the Task Force needs to be cognizant that our financial system needs a root identification artifact like an SSN and replacing it with another will divert thieves' attention to the new artifact.

We recommend the Task Force focus on reducing the exposure of the SSN to potential breaches by eliminating its use as an account or activity tracking number for everything from social security benefits to federal, state and local tax collection. All these activities alone generate millions of telephone calls and pieces of mail that contain full SSN information every year. Federal law should mandate the removal of SSN as an account number for all levels of government and private entities. Even when using the SSN as a root identification artifact, the entire SSN need not be used; a partial SSN in conjunction with other static individual information is a better authentication.

2. *Comprehensive Record on Private Sector Use of SSNs*

The Task Force, in seeking to address the extent to which the availability of SSNs to identity thieves creates the possibility of harm to consumers, is considering whether to recommend that the Task Force investigate and analyze how SSNs are currently used in the private sector, and how these uses could be modified or limited to help minimize the unnecessary exposure of SSNs and/or to make them less valuable in committing identity theft. Would such an effort be helpful in addressing the problem of identity theft? To what extent would such an effort be the appropriate way to gather this information?

Comment:

ING DIRECT does not distinguish between private and government sectors. The approach should be similar; use of SSNs by the private sector is as much of an issue as public sector use.

3. *National Data Security Standards*

The Task Force is considering whether to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. Would such national requirements be helpful in addressing any deficiencies in current data security practices? If so, what would be the essential elements of such a requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size? On a related note, please provide any comments that you may have on the costs of imposing a national data security requirement on businesses.

Comment:

National data security standards would be helpful to address the security of information in the custody of entities not in scope of existing relevant regulation, i.e. GLBA, HIPPA. However, the level of impact such standards would have on identity theft is entirely dependent on the enforcement mechanism; it is nearly impossible for an identity theft victim to identify the root breach of their information, and certainly not with sufficient evidence to hold an entity liable via civil claim. Data security issues are extremely dynamic and complex; any criminal penalties must be constructed to not impart undue risk to businesses or officers.

Improving data security nationally will involve costs to the businesses that aren't already under regulatory scrutiny for data security, but the methods and tools needed for security have been sufficiently commercialized by the industries that are. Industry expertise and commoditized tools are readily available that can provide baseline due care of data. Looking at the issue from the other angle, what future cost in consumer confidence, fraud, and law enforcement do we avoid by implementing comprehensive data security? In any case, in our view it is the responsibility of any entity that collects or uses consumer data to sufficiently protect that data.

4. *Breach Notice Requirements for Private Sector Entities Handling Sensitive Consumer Information*

The Task Force is considering whether to recommend that a national breach notification requirement be adopted. Would such a breach notification requirement be helpful in addressing any deficiencies in the protocols currently

followed by businesses after they suffer a breach? If so, what would be the essential elements of such a national breach notification requirement? Does the need for such a national standard, if any, vary according to economic sector, business model, or business size?

Comment:

A federal statute on data breach notice would be a benefit to business only if it takes precedence over state and municipal statutes to eliminate the need to track and comply with a myriad of potentially different rules. Any privacy breach notification legislation would need an explicit definition of breach including: data involved and level of acceptable mitigating controls; well defined triggers for notification, such as whether there is likely access or abuse of the information; reasonable notification timeline expectations; and clearly stated requirements that sub-contractors report to the contracting entity. These baseline standards should be achievable by any size business in any sector.

5. *Education of the Private Sector and Consumers on Safeguarding Data*

The Task Force is considering whether there is a need to better educate the private sector on safeguarding information and on what private sector entities should do if they suffer a data breach. Additionally, the Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft, through a national public awareness campaign. Are such education campaigns an appropriate way in which to address the problem of identity theft? If so, what should be the essential elements of these education campaigns for the private sector and consumers?

Comment:

ING DIRECT feels that the financial sector has ample material and knowledge regarding data breach response. The most effective motivator for the private sector will be specific requirements. Data security methods and tools could be summarized in the context of these base requirements in an informative business packet and made available through SBAs, BBBs, FTC, business lenders, advisors, and consultants.

Consumers are the ones that require the most urgent education on preventing identity theft. Home PCs and broadband connectivity are available at prices that are acceptable to all socio-economic levels; identity theft and fraud perpetrators are targeting those who are not savvy with the use of these new tools. A strong push should be made to ensure that personal computers that are the typical repositories of personal information should be sold with full protections; this can be achieved either via strong and explicit customer warnings at the point of purchase or by mandating the inclusion of instructional content on protecting your identity online and in real life. Community educational programs can deliver similar content; early education in the public schools will help tomorrow's online consumer be prepared. The government needs to recognize the importance of

safeguarding data and consider it an integral part of early education and work with the Dept. of Education and local school districts to pilot education programs.

II. PREVENTING THE MISUSE OF CONSUMER DATA

The Task Force is also considering how to make it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities. In its interim recommendations to the President, the Task Force noted that developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information. The Task Force accordingly recommended that the Task Force hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. Those workshops will begin in early 2007. Are there any other measures that the Task Force should consider in addressing how to prevent the misuse of consumer data that has fallen into the hands of an identity thief?

Comment:

We believe the Task Force should consider the workshop scope to include identifying the best means of preventing misuse of consumer data and not just focus on authentication. An initial step is to ensure that thieves cannot easily obtain the information, but in the unfortunate event information is compromised, there are steps all institutions must take to make it more difficult for the thief to perpetrate fraud and identity theft. The second layer of defense exists within a secure authentication scheme that goes beyond the basic login & password type of authentication, and the FFIEC guidance on *Authentication in an Electronic Banking Environment* somewhat addresses this. Biometrics, knowledge-based "out of wallet" questions and/or improved identity vetting processes with data analysis will help deter these incidents from occurring. Direct verification of SSNs through the SSA could also help in ensuring financial institutions are interacting with the correct individual.

The adherence to these enhanced authentication standards prior to account openings or during maintenance of accounts and "high risk" transactions is expected to reduce the instances of perpetrated fraud using identity theft as the vehicle. We recommend a national registry of identity theft victims and providing financial institutions the ability to utilize this information during account opening and maintenance processes to enhance the protection of consumer assets. ING DIRECT strongly supports all efforts to enhance the protection of consumers and recommends the workshops occur periodically in order to address emerging practices and risks.

III. VICTIM RECOVERY

The Task Force has been considering the barriers that victims face in restoring their identity. The Task Force has specifically addressed the following issues:

1. *Improving Victim Assistance*

The Task Force is considering ways in which to provide more effective assistance to identity theft victims, including, but not limited to, providing training to local law enforcement on how best to provide assistance for victims; providing educational materials to first responders that can be used readily as a reference guide for identity theft victims; developing and distributing an identity theft victim statement of rights based on existing remedies and rights; developing nationwide training for victim assistance counselors; and developing avenues for additional victim assistance through the engagement of national service organizations. Would these measures be effective ways to assist victims of identity theft? Are there any other ways to improve victim assistance efforts that the Task Force should consider?

Comment:

It is important to support the victims of identity theft in a manner that minimizes the effort to recover and reduces the disruption to their daily lives. The Task Force needs to review the best practices offered by financial institutions at the forefront of combating identity theft. These practices, techniques or forms, etc. may be used to improve the capabilities of smaller institutions or become the standards a national service organization tasked with victim assistance uses. We recommend there be a central government or other organization tasked with victim assistance, along with recording of instances and information sharing across institutions and industries, such as banks and insurance companies.

The most important tool to assist victims to recover is the ability to easily and comprehensively put a freeze on any further fraudulent activity dealing with the provision of credit or identifying documents (i.e. duplicates or lost drivers licenses or credit cards).

2. *Making Identity Theft Victims Whole*

The Task Force has issued an interim recommendation that Congress amend the criminal restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in attempting to recover from the effects of the identity theft. Are there other ways in which the government can remove obstacles to victim recovery?

Comment:

ING DIRECT strongly supports all legal changes to further protect victims and provide disincentives to thieves. We support the specific changes proposed by the Dept. of Justice and further suggest that any restitution program be part of a criminal prosecution process. The Task Force needs to consider that restitution will most often not be sufficient to offset legal counsel and court fees and therefore not used if it is the responsibility of the consumer to independently seek restitution through civil action.

3. *National Program Allowing Identity Theft Victims to Obtain an Identification Document for Authentication Purposes*

To give identity theft victims a means to authenticate their identities when mistaken for the identity thief in a criminal justice context, several states have developed voluntary identification documents, or "passports," that authenticate identity theft victims. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an "Identity File." The Task Force is considering whether federal agencies should lead an effort to study the feasibility of developing a nationwide system that would allow identity theft victims to obtain a document or other mechanism that they can use to avoid being mistaken for the suspect who has misused their identity. Would such a system meaningfully assist victims of identity theft? If so, what should be the essential elements of such a nationwide system?

Comment:

The Task Force is proposing an alternative authentication mechanism for identity theft victims and using new credentials, beyond the usual existence of a driver's license and knowledge of basic information, name, address and social security number. The effectiveness of a "passport" or any other identification form system will depend on the ability of identity theft perpetrators to utilize technology and easily replicate such documents. In recent years identity theft perpetrators have utilized simple desktop computing technology to successfully replicate a diverse number of documents, from social security cards, utility bills, driver's license and pay-stubs, to mention a few. The person requesting and obtaining these documents from such as system would need strong authentication to prevent the unauthorized access to consumer information.

From a financial institution perspective the identity of customers is ensured through Know Your Customer processes that are based on systems and technology that ensure the person can correctly respond to knowledge-based or "out-of-wallet" questions about themselves that perpetrators cannot easily compromise. Recent FFIEC guidance on customer authentication, which drives financial institutions to use many such techniques, has led to less reliance on documentation and more on individuals knowing enough information about

themselves as information exists in external sources, such as credit bureaus and non-credit bureau information sources.

We are in favor of systems to support victims of identity theft, but we believe the Task Force needs to focus on preventive measures.

4. Gathering Information on the Effectiveness of Victim Recovery Measures

To evaluate the effectiveness of various new federal rights that have been afforded to identity theft victims in recent years, as well as various new state measures to assist identity theft victims that have no federal counterpart, the Task Force is considering whether to recommend (a) that the agencies with enforcement authority for the Fair and Accurate Credit Transaction Act (FACT Act) amendments to the Fair Credit Reporting Act assess the amendments' impact and effectiveness through appropriate surveys or other means, and (b) that agencies conduct an assessment of state credit freeze laws, including how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. Are such studies important for formulating a national strategy on how to combat identity theft? Are there any other evaluations that should be done to assess the effectiveness of victim recovery measures?

Comment:

These studies are essential to identify the effectiveness of programs and regulations and should be conducted on an ongoing basis. Government agencies should ensure that the opinions and views of industry stakeholders are taken into consideration in formulating future tactics and amending the current tactical measures taken.

IV. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The May 2006 Executive Order stated that it shall be the policy of the United States to use its resources effectively to address identity theft, including through "increased aggressive law enforcement actions designed to prevent, investigate, and prosecute identity theft crimes, recover the proceeds of such crimes, and ensure just and effective punishment of those who perpetrate identity theft." The Task Force has accordingly examined various ways, including the following, by which this goal can be achieved.

1. Establish a National Identity Theft Law Enforcement Center

The Task Force is considering whether to recommend the creation of a National Identity Theft Law Enforcement Center, to better coordinate the sharing of

information among criminal and civil law enforcement and, where appropriate, the private sector. Such a Center could become the central repository for identity theft complaint data and other intelligence from various sources received by law enforcement, as well as a hub for analysis of that information. The analyses could be used to provide support for law enforcement at state and federal levels in the investigation, prosecution, and prevention of identity theft crimes. The Center also could develop effective mechanisms to enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information through remote access. The Center could also assist investigative agencies, before they begin a particular investigation, in determining whether another agency is already investigating a particular identity theft scheme or ring. Would the establishment of such a Center assist law enforcement in responding to identity theft? If so, what should be the core functions and elements of that Center?

Comment:

ING DIRECT supports the creation of a single national organization tasked with combating identity theft. The fragmented approach by various government agencies in investigating identity theft cases and dispersion of information has been an impediment in preventing and resolving identity theft cases. ING DIRECT believes that a single information source that will include all known identity theft victim information and will share such information with industry stakeholders is a critical component of identity theft prevention. Such an entity would need to be sufficiently staffed and funded to achieve its intended goals. Relying on thinly staffed law enforcement agencies and setting thresholds and criteria for prosecution and investigation will lead to failure.

Similar to what the FBI refers to as the "Identity File," this entity should establish rules so that all identity theft information is captured nationwide and shared with all federally chartered and insured financial institutions. These institutions may choose to utilize this list similar to the OFAC list and make it part of a risk-based customer screening process, subsequently limiting the opportunity for identity thieves. Inter-agency communication will improve efficiency, reduce investigation time thus limiting potential damage to consumers, and increase conviction rates.

It is well known that the Federal Trade Commission (FTC) and the FBI maintain their own victim data lists and are unwilling to share this information with financial institutions. This is a prime opportunity for the government to leverage the available information by sharing with more stakeholders. This would make the federal government an enabler and not a bottleneck in the war against identity theft.

2. *Ability of Law Enforcement to Receive Information from Financial Institutions*

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force is considering:

(a) whether the Justice Department should initiate discussions with the private sector to encourage increased public awareness of Section 609(e) of the Fair Credit Reporting Act, which enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf;

(b) whether relevant federal law enforcement agencies should continue discussions with the financial services industry to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft; and

(c) whether the Justice Department should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report.

Would such measures meaningfully assist law enforcement efforts in combating identity theft and/or meaningfully assist in forming partnerships between law enforcement and the private sector? Are there any other measures that could be implemented to strengthen the relationship between the private sector and the law enforcement community in responding to identity theft?

Comment:

ING DIRECT supports open communication and information sharing with the private sector. We further support making information sharing mandatory from the private sector to a single national agency that coordinates identity theft prevention and information. The coordination of efforts across government, financial institutions and credit bureau agencies is critical. All suggested approaches are proposals in the correct direction, and there needs to be a strong push beyond discussions to enable and mandate the sharing on information in this area for the protection of consumers.

3. *Prosecutions of Identity Theft*

The Task Force is considering whether steps can be taken to increase the number of state and federal prosecutions of identity thieves, including (a) requiring each United States Attorney's Office to designate an identity theft coordinator and/or develop a specific Identity Theft Program for each District, including evaluating

monetary thresholds for prosecution, (b) formally encouraging state prosecutions of identity theft, and (c) creating working groups and task forces to focus on the investigation and prosecution of identity theft. Would these measures meaningfully assist in increasing the number of identity theft prosecutions? Are there any other measures that can be implemented that would increase state and federal prosecutions of identity thieves?

Comment:

ING strongly supports prosecuting perpetrators of identity theft regardless of monetary thresholds. Currently authorities use monetary thresholds in the decision to pursue or not pursue prosecution; this leaves many identity thieves unpunished as they intentionally operate below the “radar” or simply collect and broker stolen identity theft information. The federal government needs to reconsider the monetary thresholds and ensure if any such thresholds exist they fit within a national strategy to combat identity theft. In order to interrupt the cycle of identity theft the “distribution network” needs to be addressed as well.

Thank you again for the opportunity to provide comments on the Identity Theft Task Force Request for Public Comment. If you have any questions, please contact Peter Aceto, 302-255-3888.



Peter Aceto
Chief Risk Officer and Chief of Staff
ING DIRECT USA