

Coalition for Data Security

January 19, 2007

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



Re: Identity Theft Task Force, P065410

To Whom It May Concern:



This letter is submitted on behalf of the Coalition for Data Security (“Coalition”) in response to the request for comment on a variety of topics (“Request”) issued by the federal Identity Theft Task Force (“Task Force”). The Coalition appreciates the opportunity to provide its comments to the Task Force.



What Is “Identity Theft”?

The Task Force’s Request touched on a variety of topics relating to “identity theft,” yet the Request did not specifically define what the Task Force believes comprises actual “identity theft.” Nor did the Task Force define the harm as part of its Interim Recommendations. The Coalition believes that the Task Force, if it is to propose measures to address identity theft, should also determine the scope of the crime.



In particular, we are concerned that the use of over-broad definitions of “identity theft” is a disservice to consumers because such definitions tend to detract from the severity of actual identity theft. This is true because other crimes, such as credit card fraud, are routinely classified as “identity theft” crimes. The Coalition is well aware of the harms and costs to consumers associated with credit card fraud and similar crimes, but they do not rise to the level of true identity theft. True identity theft—a circumstance in which a criminal is able to open new accounts in the victim’s name—is a limited and well defined problem. Furthermore, identity theft is a much more pernicious crime deserving of dedicated and focused federal attention and resources.



A case in point is the recent trend to categorize data breaches as a key risk factor contributing to identity theft. In fact, data breaches generally do not result in consumer harm. To the extent harm results, it is generally limited to account-level fraud, not identity theft. We are attaching two studies, one by ID Analytics and the other by the Javelin Strategy and Research, for review by the Task Force further describing this and related issues. We hope these are useful to the Task Force in its effort to define identity theft.



Use of SSNs

The relationship between Social Security Numbers (“SSNs”) and identity theft is complex. The SSN is a tool in identity theft schemes only because it is a critical protection against identity theft. Stated differently, because SSNs are so effective at preventing identity theft, if a criminal can compromise an SSN he or she is able to attempt to commit fraud through its use. Although use of SSNs has been blamed in connection with identity theft, the truth is that SSN is an additional piece of information used by government agencies, financial institutions, and others to protect against fraud and ensure the accurate matching of information with existing records. Any solution toward identification authentication would be based on *increasing* the information available to verify consumer identity, not *reducing* the information available.



We understand the Task Force’s desire to understand how public and private sector entities collect and use SSNs. This is a laudable goal, but one that is likely going to be difficult to achieve. We also understand the Task Force’s apparent belief that if SSNs are collected and used only for legitimate and appropriate purposes, perhaps there will be less of an opportunity to compromise SSNs. We agree—but believe the solution is proba-

Coalition for Data Security

bly the creation of data security requirements around certain databases, such as those that contain a consumer's name and SSN. (See below.) While there may be slightly incremental gains that could be made with respect to protecting SSNs if their collection and use were limited to only "legitimate" reasons, we believe it will be extremely difficult to draw a bright line between legitimate reasons and illegitimate reasons. Furthermore, if the Task Force attempts to delineate between permissible and impermissible current and future uses of SSNs, the consequences of any misjudgment could far outweigh any benefits such delineation could provide. This is not to say that there may not be some obvious reforms. We caution the Task Force, however, on proceeding beyond only the most "surefire" ones.

Data Security

The need to review the use and collection of SSNs—or any other sensitive consumer information—could be mitigated through the implementation of effective data security protections in the public and private sector. The Coalition is a strong proponent of establishing appropriate data security requirements with respect to sensitive consumer information, such as consumers' names coupled with SSNs and/or financial account numbers. Indeed, we believe that this is perhaps the best approach toward protecting SSNs and other important information: government agencies and private sector entities should have reasonable programs designed to protect the security of sensitive consumer information. If this goal is achieved questions about the collection and use of SSNs will become less critical.

Currently, financial institutions must protect "nonpublic personal information" under the Gramm-Leach-Bliley Act ("GLBA"). We believe that the federal banking agencies and the Federal Trade Commission ("FTC") have done an admirable job in crafting data security requirements that provide a flexible, risk-based approach to data security. The Coalition believes that these requirements could be easily adapted to apply to other entities that possess sensitive consumer information, keeping in mind some of the existing protections that are in place today. For example, we believe the appropriate agencies should consider whether compliance with private sector data protection schemes, such as the Payment Card Industry Data Protection Standard, may be sufficient in lieu of complying with any new federal standard. Such an approach would improve data security requirements dramatically and assist in preserving the integrity of sensitive consumer information.

Having said this, we believe that the focus of any data security requirement should be on computerized data. We do not believe that there are significant benefits to be gained by requiring the public and private sectors to completely revamp their existing paper records systems. Rather, it would be much more efficient and effective to focus on computerized information since the nature of such information makes it more vulnerable to widespread compromise.

Breach Notification

The Coalition is also a strong supporter of appropriately tailored national uniform federal data breach notification requirements. In general, we believe that consumers should receive a notice of a data breach in those limited circumstances in which they are at a significant risk of harm. Furthermore, such a requirement should be subject only to federal administrative enforcement. We also support efforts to deem financial institutions who are in compliance with existing GLBA requirements to be in compliance with any new federal law. In this regard, there is general agreement that the GLBA standard is sufficient from a consumer protection standpoint, and financial institutions should not be required to redesign their existing compliance programs. We attach the testimony of Karl Kaufmann on behalf of the U.S. Chamber of Commerce before the House Subcommittee on Financial Institutions and Consumer Credit for the record in support of our position.

Credit Freeze

We applaud the Task Force for its proposal to gather and evaluate existing and potential tools to assist identity theft victims. In particular, the Task Force "is considering whether to recommend that the agencies with enforcement authority for the [FCRA] assess the [FACT Act's] impact and effectiveness..., and that agencies

Coalition for Data Security

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.” We strongly believe that a realistic and thorough assessment of both of these topics is critical if the Task Force (or any other entity) seeks to improve assistance for identity theft victims.

The enactment of the FACT Act in 2003 was a significant step forward with respect to identity theft prevention and mitigation. The Bush Administration was instrumental in ensuring that effective and robust consumer protections were included in the legislation. It is only appropriate for the Task Force to conduct an inventory of those improvements and assess their effectiveness. For example, as a result of the FACT Act, identity theft victims now can:

- Block the reporting of inaccurate information by a consumer reporting agency;
- Block the furnishing of inaccurate information to a consumer reporting agency;
- Obtain information and records from businesses that interacted with the identity thief;
- Insert an extended fraud alert in their files at consumer reporting agencies, and receive a free file disclosure from the consumer reporting agency in connection with the fraud alert;
- Obtain a detailed and comprehensive summary of their federal rights from a consumer reporting agency;
- Prevent the sale or transfer of a debt relating to their identity theft; and
- Obtain information from a debt collector attempting to collect on the fraudulent debt.

These tools, when evaluated on the whole, are obviously powerful and significant. We have been surprised, frankly, at the lack of attention these improvements in the law have been given by the Bush Administration and the legislators who authored them. We urge the Task Force to consider the effectiveness of these and other identity theft victim mitigation measures before determining what additional laws are needed.

In particular, a thorough assessment of existing remedies is critical before determinations are made with respect to the advisability “credit freeze”. The stated intent of a credit freeze law is to make it impossible for a criminal to obtain credit in the name of someone who has placed a “freeze” on his or her file at a consumer reporting agency. The criminal is unable to obtain credit in this circumstance because the creditor is unable to access the intended victim’s “frozen” credit report, and the creditor will therefore almost certainly decline the application. Naturally, the individual who placed the freeze on his or her file is also unable to obtain credit for the same reason. Given the strong protections identity theft victims receive as a result of placing an extended fraud alert in their file, credit freeze laws are overkill. A credit freeze imposes severe repercussions that result in more harm than good to many consumers.

We commend the Task Force for deciding to evaluate existing remedies for identity theft victims and state credit freeze laws. It is imperative, however, for the Task Force to evaluate state credit freeze laws in a comprehensive and objective manner. In so doing, the Task Force should not only review the purported effectiveness of freeze laws and their costs, but also the significant hurdles consumers face in obtaining various products and/or services once they freeze their file with a consumer reporting agency. Any evaluation should consider the technical and practical impediments inherent to the process of lifting a freeze. For example, consumers who place a freeze on their file have difficulties in obtaining instant credit due to the logistics involved in “thawing” the file. This is particularly troubling for low-income consumers who need to make an emergency purchase, such as the replacement of a refrigerator, and do not have the ability to make the purchase without obtaining instant credit.

Credit freezes also thwart consumers’ ability to obtain other types of services, including other forms of credit, unless those consumers have the time and foresight to “thaw” their file in connection with their credit application. We strongly urge the Task Force to review, just as one example, the difficulties consumers face in connection with locking in a mortgage rate and applying for a new mortgage if they have frozen their file at a consumer reporting agency.

Although we are confident that the Task Force would consider the obvious costs associated with credit

Coalition for Data Security

freeze laws—such as those associated with the regulatory burdens and lost sales—we also believe the Task Force should consider the broader impact freeze laws would have on the nationwide credit granting system the Bush Administration and vast majority of legislators touted as part of the enactment of the FACT Act. The United States has the most robust credit market in the world, in part, as a result of the market’s speed and efficiency. Credit freeze laws threaten this critical component of our financial infrastructure. We strongly urge the Task Force to engage in an in depth review of this issue.

We strongly believe that the tools provided to identity theft victims as a result of the FACT Act are sufficient to provide meaningful assistance in the wake of identity theft. If the Task Force believes that state credit freeze laws may provide further assistance to such victims, we strongly urge the Task Force that, any credit freeze law should be available only to identity theft victims. A credit freeze is indisputably the “nuclear option” with respect to identity theft mitigation. It may be that the Task Force determines that there are circumstances in which identity theft victims should have the option to exercise this “nuclear option.” The severity of the remedy, however, makes it unsuitable in our opinion for use by consumers as an identity theft prevention measure. We were therefore particularly troubled by the Task Force’s Interim Recommendations that suggested consumers should consider using state credit freeze laws as a first line of defense against identity theft, especially in the wake of certain data breaches. Not only do we think that reliance on credit freezes as a preventative measure is unwise for the reasons described above, but we are also aware of various independent studies suggesting that data breaches generally do not pose significant risks of identity theft. Given the findings in these studies that data breaches generally do not pose a significant risk of identity theft, we believe that a recommendation to consumers to use credit freezes if they receive a data breach notice is ill advised absent other aggravating factors such as the actual compromise of an individual’s identity.

Law Enforcement

As a general matter, the Coalition strongly supports giving law enforcement the tools necessary to fight and prosecute identity theft. In many instances, law enforcement simply does not have the necessary resources to pursue identity theft crimes resulting in criminals remaining on the street and a lack of deterrence to the crime. The Task Force is apparently considering whether to recommend the creation of a National Identity Theft Law Enforcement Center (“Center”) to coordinate the sharing of criminal and civil law enforcement and “where appropriate” the private sector. The Coalition supports the concept of a Center to act as a clearinghouse of sorts for identity theft information. We note that in order for the Center to be effective, it must be a two-way street between law enforcement and the private sector. We caution the Task Force against the creation of a Center which serves only as another regulatory burden without giving private sector companies the identity theft prevention and mitigation benefits associated with a clearinghouse. We are therefore supportive of the Task Force’s consideration of increasing the number of federal and state identity theft prosecutions and special enforcement initiatives.

Coalition for Data Security

The Task Force is also considering proposals with respect to receiving information from the private sector. The Coalition believes that law enforcement probably has sufficient ability to gather most information necessary in connection with identity theft crimes, such as under the Fair Credit Reporting Act, the Right to Financial Privacy Act, and other laws. To the extent additional authorizations are necessary, the Coalition asks that the Task Force recommend that financial institutions be given a safe harbor for providing such information to law enforcement.

The Coalition appreciates the opportunity to share these comments. Please do not hesitate to contact me at [the number listed above] if we can provide any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "Jeffrey A. Tasse". The signature is written in a cursive style with a long, sweeping tail on the final letter.

Jeffrey A. Tasse
Executive Director

Coalition for Data Security

Footnotes

The Coalition is comprised of financial institutions and businesses that use consumer credit information to deliver credit to the widest possible range of consumers more quickly and cheaply than in any other country in the world. Coalition members are highly competitive and innovative businesses that have played a lead role in the transformation of global and domestic commerce. Without their expertise in the production and delivery of consumer credit, internet commerce would not exist.

³Requirements for consumer reporting agencies to “thaw” files quickly are of little use in many circumstances, since consumers are not necessarily in a position to call a consumer reporting agency, authenticate their identity, and request a thaw at the time many purchases are made.

²This list does not include the numerous identity theft prevention (as opposed to mitigation) measures enacted as part of the FACT Act.

See, e.g., “Data Breaches and Identity Fraud: Misunderstanding Could Fail Consumers and Burden Businesses,” Mary T. Monahan, Javelin Strategy & Research, August 2006 and “National Data Breach Analysis,” ID Analytics, January 2006.