

FEDERAL IDENTITY THEFT TASK FORCE

Attorney General Alberto Gonzales Federal Trade Commission Chairman Deborah Platt Majoras.

On May 10, 2006, the President signed an Executive Order establishing an Identity Theft Task Force, and directing it to develop a coordinated strategic plan to combat identity theft. The Task Force was specifically directed to make recommendations on ways to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. The Executive Order directed the Task Force to deliver the strategic plan to the President within 180 days. By further Executive Order, issued November 3, 2006, the President amended the original order to require submission of the strategic plan by February 9, 2007, or as soon as practicable thereafter as the Chairman and Co-Chairman shall determine.

On September 19, 2006, the Task Force published Interim Recommendations, which can be found at www.ftc.gov/opa/2006/09/idtheft.htm.

The Task Force, in working to produce a final strategic plan to the President, is considering, among other things, various ways to improve the coordination and effectiveness of criminal prosecution of identity theft; to enhance data protection for sensitive consumer information maintained by the public sector, private sector, and consumers themselves; to provide more comprehensive and effective guidance for consumers and the business community; and to improve recovery and assistance for consumers following a breach or misuse of their information. The Task Force members have focused their work on the following four areas:

! Keeping sensitive consumer data out of the hands of identity thieves through better data security practices and by educating consumers to protect themselves;

- ! Making it more difficult for identity thieves, when they are able to obtain consumer data, to use the information to steal identities;
- ! Assisting the victims in recovering from crime; and
- ! Deterring identity theft by aggressively prosecuting and punishing those who commit the crime.

Although there is no legal requirement that the Task Force formally solicit public comment, the Task Force believes that seeking further comment on these issues will supplement the research and analysis already conducted, provide further information about the proposals it is considering, and identify areas where additional recommendations may be warranted. It is not expected that the Task Force will respond directly to particular comments or suggestions. Rather, the Task Force will use submitted comments to supplement the outreach and analysis already conducted. The Task Force invites comments on the following issues and questions:

Problem Summary:

The problem of identity theft is a difficult issue to tackle due to the ease of committing the crime, lack of training to proper entities, lack of community engagement regarding the issue and cooperation on several levels.

In order to effectively tackle the problem of identity theft all parties need to work together effectively, all at the same time, and all at the same pace. This is almost insurmountable, as each party tends to try to address the problem on their own. In order for us as a society to progress in the prevention and detection of identity theft, we need to work together. This would include the government, law enforcement, financial industry and private businesses.

Some of the problems we are facing have been outlined below to give you an understanding of the issues presented.

Financial Industry: The banking system is continually revising and improving the security features on credit cards to help combat the fraud. But for this to be truly effective, their business clients need to be properly trained on what the features are, how to verify them, and the technology available to identify counterfeits/altereds, which is currently not being offered. Banks, credit unions and any financial institution that provides merchant services to businesses should be required to provide training sessions of this nature. Financial institutions should also be providing identity theft prevention sessions to their customers as part of their efforts and contribution to the communities in which they serve.

Law Enforcement: Due to the overwhelming incidence of identity theft, law enforcement agencies are suffering the inability to take all reports requested. This is also due to lack of training for desk personnel to identify the crime as a criminal matter and not a civil matter. Many victims are turned away because of this lack of understanding. They are told it is a civil crime and they will have to file in small claims court. There is also a lack of knowledge amongst patrol officers on how to identify the elements of the crime. Detective and investigative personnel are very well versed on the subject nature, as they are the investigators. But when it comes to the patrol forces, the ones who take the initial report, there is an issue.

Another issue law enforcement faces is the need to place a dollar limit on cases to be filed. Because they are overwhelmed the dollar limit is placed to help weed out cases in an effort to reduce caseload. When a case meets or exceeds that dollar limit, then the crime is investigated. This also spills over into the district attorney's office as many have also set their own dollar limit on cases they will file.

Additionally, the penalties are not severe enough that they are considered a threat to the criminal. Why would a criminal want to rob a bank and use a weapon (which will add an enhancement to his sentence for the use of the weapon) and risk going to prison when he can easily commit some type of identity theft, which carries for the most part, a slap on the wrist?

Private Businesses: These businesses that accept credit cards as a form of payment, are not receiving training from their financial institutions on how to recognize the fraud. Additionally, these businesses are not providing training to their employees, specifically front line employees, on what to look for, how to detect, and what to do if they detect fraud. If it is easy for the criminal to pass their counterfeit/altered documents then the cycle will continue. We must harden the target at all levels and at all points.

Government: There needs to be a push from the government to hold businesses accountable that use SSN for identification purposes. SSN were never intended to be a form of identification. They were meant for social security and retirement benefits. That's it. But due to the lack of any form of identification, society started using this number to verify identity. Why? Because this is the only number issued to an individual that never changes within their lifetime. Since the closest thing to a legal identification is a driver's license or identification card, business started using those to verify identity. However, a driver's license is just that. It is a document that gives the holder the permission to drive a vehicle. It in no way, shape or form verifies their identity. The Department of Motor Vehicles does not verify identity when these documents are issued. Viewing a paper copy of a birth certificate, social security card or other form of identification is not authenticating the document to verify

identity. The Real ID Act may change some of this once it is implemented at the Department of Motor Vehicle level.

Consider this: I am a criminal. I want to create a new identity for myself so I can go shopping. I will search death certificates for someone who would be about my age if they were still alive and has been dead approximately 7 to 10 years. Why 7 to 10 years? Because that is when that deceased person's credit record will be clean. I will then order a copy of the death certificate. Once I obtain that, I will order a copy of their birth certificate. My next trip, to the Department of Motor Vehicles to get my new driver's license or identification card. Then on to the Social Security Office to obtain a copy of my social security card. After that, it's clear sailing. I can obtain credit and start my spending spree.

I. MAINTAINING SECURITY OF CONSUMER DATA

The Task Force Interim Recommendations addressed data security in the public sector by calling for examination by federal agencies of their collection and uses of Social Security numbers (SSNs), the piece of information that is often most effective in committing identity theft. The Task Force also recommended that the Office of Management and Budget conduct a survey to assess how well agencies protect the sensitive consumer data they maintain, and recommended that the Office of Personnel Management identify and eliminate the gratuitous use of SSNs in human resources forms used by federal agencies. The Task Force is considering whether additional measures, including the following, should be taken to further enhance the protection of sensitive consumer information and thus keep it out of the hands of identity thieves:

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? *The use of SSNs by government entities should be very limited in nature. If the SSN is used by an entity, it should be maintained only in the private files within that entity. No SSN should ever be used on any identification or CAG card. Understanding that certain government entities do need to know the SSN of employees and such, it does not have to be placed on a document which may be viewed by many others or easily lost. Currently, there is no point to having SSN on these types of cards as most locations that number is not verified anyway. The card is viewed to visually compare the photo to the card presenter.* On a related issue, please provide any comments that you may have on what information could be used as a substitute for SSNs. *The use of an employer issued identification number as proposed in the recommendations could be effective. However, keep in mind that data breaches to obtain these numbers are still a risk. One would assume that if an employer issued their own identification numbers, their computer files would cross reference that number with the individual's SSN and thus if a breach is experienced, the criminal would still be able to obtain the SSN. I do however believe that the use of an employer issued number can be very effective in regards to the SSN being viewed on the card out in public. It could not be seen accidentally or intentionally over someone's shoulder. A dishonest employee would not be able to copy another person's SSN, which often happens to commit the crime. However, even placing an employer issued number on certain documents such as identification or common access cards as the military does, is not needed unless it is verified at the point of access or when viewed to confirm identity. Barcodes, microchips, smart cards or some other type of method that does not allow the ability*

for someone to visually view the feature and use it criminal is highly desirable. Both options of using SSNs and employer issued numbers present this problem.

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? *I do believe that this undertaking would be extremely beneficial in limiting the use of SSNs in the private sector. Most businesses that ask or require a SSN for their files never actually use that information. They just want to have it in their files as a form of identification. This is pointless since they do not verify the SSN. A large portion of identity theft crimes occurs by dishonest employees. Someone who works at a doctor's office, financial institution, auto dealership, etc. who peruses the client files to copy down SSN numbers.* To what extent would such an effort be the appropriate way to gather this information? *The outcome of this type of investigation and analysis would help to possibly structure some governmental guidelines or restrictions on the type of information businesses may obtain from their customers. Just as the Taskforce has recommended reviewing the use of SSNs in government agencies to determine where they can eliminate, restrict, or conceal their use, can also be beneficial in the private sector.*

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? *I think this would be something that if imposed, would be impossible to enforce due to the number of businesses that collect such data. The cost of implementing something like this would most likely be astronomical and infeasible. A more appropriate approach might be to institute some type of penalty for businesses if a customer can prove that their information was comprised by that particular business or due to the businesses lack of diligence in protecting their client's information. Holding the business accountable by a penalty or fine if their confidential information is breeched could possibly be an effective compliance tool.* Does the need for such a national standard, if any, vary according to economic sector, business model, or business size? **Yes** On a related note, please provide any comments that you may have on the costs of imposing a national data security requirement on businesses.

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? **No comment.**

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? *Yes, Yes, and Yes!!! This is the missing piece to the prevention puzzle. Currently most of the efforts are reactionary. We need to be proactive and follow the Crime Element Triangle model by removing the opportunity for the crime to occur by educating the masses. How can we expect to deter this type of crime if the private sector and consumers are not educated? They are the victims and we need to target them in the efforts to help combat this crime. Our company continually teaches these types of classes and has had several attendees tell me they had no idea how these crimes are being committed and how easy it is. They are better armed to protect themselves and wind up realizing that they have just as much a responsibility to stop this type of crime as the government, law enforcement and business community does. But this public awareness campaign needs to be done on the street level, offering community wide trainings all across the nation. Have the key stakeholders in communities sponsor these training. This would be the banking institutions, local municipal offices, community groups, government entities, churches, professional associations, etc. These trainings cannot be combined. Separate sessions for consumers and the private sector need to be conducted as a different approach and information would be provided in each session.*

If so, what should be the essential elements of these education campaigns for the private sector and consumers?

Consumer: *They need to know the ways criminals are getting their personal information. The many different schemes and cons need to be explained to them so they will be able to identify them. Consumers need to know how they can protect themselves besides just checking their credit report (which is not completely effective). Items take up to 6 months to show up on a credit report and then it is too late. The average identity theft victim does not learn of the crime for 6 months. Educating them to do other things such as checking their bank accounts and credit card statements weekly can be a faster way to detect the crime. They also need to be made aware that protecting their identity is something that they can do on their own without hiring a third party. Many new businesses have popped up and are charging consumers for something they can easily do themselves. This is also another way to limit access to their personal information as they would not be required to give their information to a third party where there might be another opportunity for a breach to occur. They also need to be educated on what they can do if they do become a victim, what their rights are, what to file and who to contact.*

Private Sector: *They need to learn how criminals are using the information they obtain. Businesses need to be made aware that it is their responsibility to protect their client's information. Education should include how the criminals are getting the information, how they manufacture the counterfeit and altered documents and how to detect those documents. Often times people/businesses don't realize that credit card fraud, check fraud, or false identifications are a form of identity theft. This fact is not often identified by many training entities. You can even throw counterfeit currency into the mix because if they committing this crime, they are most likely also committing identity theft. We find that these types of criminals are often committing more than just one crime at a time. Businesses also need to be made*

aware of the technology that is out there to help detect counterfeit and altered documents such as ultraviolet technology. If these businesses don't learn how to detect fraud at the point of sale or point of transaction, then we are defeating the purpose. If it continues to be easy for the criminal to commit this crime in the private sector, then what use are any of our other efforts?

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. *This may not be as easy or effective as believed. How does this address all the identity theft that is committed without using someone's SSN? How does this effectively combat skimming fraud? If a criminal skims credit card information, makes their own counterfeit card using a legitimate number and then uses it around town, how does this authentication process help that? It doesn't, because all credit cards are processed via the credit card number. So if the number is legitimate on a counterfeit card, it is useless. The same holds true for check fraud. The criminal makes fraudulent checks using legitimate account numbers. Again, all banks process checks via the account number. Unless you intend on changing the way ALL financial institutions process payments, this would not be effective. It goes back to a training issue. Add to the picture the criminal's ability to obtain a good quality fake identification in down town Los Angeles*

for a mere \$250. This is where your ultraviolet technology can come in to play as it can authenticate the document itself.

In reality, it is easier to authenticate the document, whether it's credit cards, checks, driver's license, identifications, or currency, than the person's actual identity. All these documents have security features in place to help authenticate them. The problems is the people who use these documents, mainly the private sector and government, are not aware of what they are or how to check for them. 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. *I am interested in receiving more information on these workshops, as I would like to attend!!! Our company is a training company that specializes in merchant fraud and identity theft education. The continual education of our staff is a high priority for us, as we want to ensure that we stay informed.* 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?

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? *Yes, I believe these measures would be extremely effective. Many times a victim is lost and after filing a police report, has no idea what to do next. Training of the investigators and detectives who investigate these cases is crucial as they are the follow up link for the victim. If these investigators and detectives are properly trained, they can give further guidance to a victim on what to do next. Additionally, law enforcement front desk personnel as well as patrol officers also need to be trained to recognize the elements of the crime. Many times we have victims call us saying that law enforcement would not take a report. This has been due to the frontline personnel's ability to recognize it. It is not widely known, but the Office of Victim Assistance currently provides a training program to anyone who is considered a victim counselor or advocate. Partnering with their organization could be very beneficial. Developing partnerships with national service organizations and independent contractors could also be useful. These organizations could provide community workshops and trainings to help further educate consumers at large. Including financial institutions in the training program should be considered. They should be able to provide the same helpful and useful information to their clients if they become a victim.* Are there any other ways to improve victim assistance efforts that the Task Force should consider?

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? *This could be effective, however, the ability for the victim to actually receive restitution from the criminal would be very difficult. Restitution should be funded through the sale of any equipment used to commit the crime or any funds or property that was acquired through the crime.*

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? *The effectiveness of a “passport” as such should be further studied to determine the feasibility and effectiveness.* If so, what should be the essential elements of such a nationwide system?

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? *Such studies are important and should be conducted.* Are there any other evaluations that should be done to assess the effectiveness of victim recovery measures? *The fees charged to victims by credit reporting agencies needs some serious review. In most states victims are able to put a freeze or alert on their record free of charge but incur a fee when they want it removed to make a purchase. In some instances they are then charged again to re-activate the freeze or alert and are charged a fee. These services should be free of charge to victims as long as they have a police report filed and can provide the report number.*

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? ***ABSOLUTELY!!! The cross-jurisdictional boundaries that law enforcement has to deal with in regards to investigating these types of crimes is debilitating. Having the ability to share information, identify trends, and the ability to target large operating rings is much needed.*** If so, what should be the core functions and elements of that Center? ***This center could be the responsible agency for in-depth training for investigative personnel, as well as the private sector, consumers, and other governmental agencies as necessary.***

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; ***Yes!! Consumers need to be made aware of their rights. In too many cases financial institutions tell victims that they will only give information to law enforcement with a warrant. If law enforcement has to get a warrant, anywhere from 30 to 90 days to obtain, the crime and trail in most cases has gone cold by then. Identity theft criminals move on fast and usually do a good job at covering their trail. This option would be extremely helpful to law enforcement personnel and give them the ability to prepare and investigate cases faster if victims were aware that they were entitled by law to this information.***

(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 ***Yes!! The financial institutions need to stop some of their current practices such as sending convenience checks in the mail. These should be requested by the customer when wanted, not automatically sent. Credit reporting agencies need to be brought into this to because they should stop sending pre-approved credit card offers in the mail. Yet another way criminals obtain personal information.***

(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. ***I am unsure how this would be effective. All awarded credit is based on a person's credit report. What other means would businesses use to determine whom they will and won't extend credit too?***

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?

3. The Investigation and Prosecution of Identity Thieves Who Reside in Foreign Countries

To address the fact that a significant portion of the identity theft committed in the United States originates in other countries, the Task Force is considering whether there are ways that the United States can work with foreign countries to better address this problem, including:

(a) whether the Department of Justice and the Department of State should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft; **Yes**

(b) whether the U.S. Government should continue its efforts to promote universal accession to the Convention on Cybercrime and assist other countries in bringing their laws into compliance with the Convention's standards; **Yes**

(c) whether the U.S. Government should encourage those countries that have demonstrated an unwillingness to cooperate with U.S. law enforcement in criminal investigations, or have failed to investigate or prosecute offenders aggressively, to alter their practices and eliminate safe havens for identity thieves; ***This may be hard to accomplish. If these countries were already unwilling to cooperate with our efforts, way would they want to cooperate to eliminate safe havens?***

(d) whether the U.S. Government should recommend that Congress amend the language of 28 U.S.C. § 1782 and 18 U.S.C. § 2703 to clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt assistance to foreign law enforcement in identity theft cases; and **Yes**

(e) whether federal law enforcement agencies should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities. Would such measures meaningfully assist U.S. law enforcement in its ability to investigate, identify, and prosecute foreign-based identity thieves who are committing crimes in the United States? Are there any other measures that could be implemented to achieve this goal? **Yes**

4. 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, **Yes**

(b) formally encouraging state prosecutions of identity theft, and **Yes** (c) creating working groups

and task forces to focus on the investigation and prosecution of identity theft. *Yes* Would these measures meaningfully assist in increasing the number of identity theft prosecutions? *This is crucial. The relationship between District Attorney Offices', their respective cities and law enforcement regarding identity theft cases needs to be strengthened. To many times law enforcement spends many hours to prepare a case only to have the DA refuse to file due to some menial reasons. Maybe state/federal standards/guidelines on the filings of these types of cases should be considered.* Are there any other measures that can be implemented that would increase state and federal prosecutions of identity thieves?

5. Targeted Enforcement Initiatives

The Task Force is considering whether to propose that law enforcement agencies undertake special enforcement initiatives focused exclusively or primarily on identity theft, including specific initiatives focused on (a) unfair or deceptive means to make SSNs available for sale; (b) identity theft related to the health care system; and (c) identity theft by illegal aliens. Additionally, the Task Force is considering whether to recommend that federal agencies, including the SEC, the federal banking agencies, and the Department of Treasury review their supervisory and compliance programs to assess whether they adequately address identity theft and create sufficient deterrence. Would these special initiatives be useful in prosecuting and punishing identity thieves? *These are all important efforts. However, law enforcement throughout the nation is suffering from severe personnel shortages. Unless some type of funds would be available to help offset the cost of additional personnel, this might be difficult to accomplish.* Are there any other such special enforcement initiatives that could make a difference in deterring and punishing identity thieves? *A recent trend in the past few years has been to convert many law enforcement positions into civilian positions for cost savings. Sworn*

personnel cost a much higher rate than civilian. Possibly having highly trained civilian personnel assigned to law enforcement agencies to conduct most of the investigations, other than arrests, might be a feasible idea.

6. Amendments to Federal Statutes and Guidelines Used to Prosecute Identity-Theft Related Offenses

The Task Force is considering whether to recommend that Congress amend the identity theft and aggravated identity theft statutes to ensure that identity thieves who misappropriate information belonging to corporations and organizations can be prosecuted, and add several new crimes to the list of predicate offenses for aggravated identity theft offenses, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit those crimes. The Task Force is also considering whether to recommend that Congress amend 18 U.S.C. § 1030(a), the statute that criminalizes the theft of electronic data, by eliminating the current requirement that the information must have been stolen through interstate communications. Further amendments under consideration by the Task Force include:

- ! amending 18 U.S.C. § 1030(a)(5) by eliminating the current requirement that the defendant's key-logging or malicious spyware actions must cause "damage" to computers and that the loss caused by the conduct must exceed \$5,000;
- ! amending the cyber-extortion statute, 18 U.S.C. § 1030(a)(7), to cover additional, alternate types of cyber-extortion;
- ! outlawing pretexting by providing both criminal and civil penalties for such conduct;
- ! enacting legislation that would make it a felony for data brokers and telephone company employees to knowingly and intentionally sell or transfer customer information without prior

written authorization from the customer, with appropriate exceptions for law enforcement purposes;

! amending the U.S. Sentencing Guidelines to ensure that an identity thief's sentence can be enhanced when the criminal conduct affects more than one victim; and

! amending the definition of "victim," as that term is used under United States Sentencing Guideline section 2B1.1, to state clearly that a victim need not have sustained an actual monetary loss.

Would such amendments meaningfully assist prosecutors in charging, convicting, and ensuring the just punishment of identity thieves? **Yes** Are there any other potential amendments to the provisions of the United States Code or U.S. Sentencing Guidelines that the Task Force should consider?

7. Training for Law Enforcement Officers and Prosecutors

The Task Force is considering whether to recommend enhancing the training for law enforcement officers and prosecutors who investigate and prosecute identity theft offenses, including by: (a) developing a course at the National Advocacy Center (NAC) focused solely on investigation and prosecution of identity theft; (b) increasing the number of regional identity theft seminars hosted by the U.S. Postal Inspection Service, Justice Department, Federal Trade Commission, U.S. Secret Service, and American Association of Motor Vehicle Administrators;

This should also include each states entity responsible for police officers standards such as Peace Officers Standards and Training (P.O.S.T.) in the state of California. These are the entities that most law enforcement receives the majority of their training from. (c) increasing

resources for law enforcement available on the internet, including by ensuring that an Identity Theft Clearinghouse site could be used as the portal for law enforcement agencies to gain access

to additional educational materials on investigating identity theft and responding to victims; and (d) reviewing curricula to enhance basic and advanced training on identity theft. Are these measures necessary or helpful to law enforcement officers and prosecutors? *Absolutely!!! For the past two year's we have held training conferences specifically for investigators and detectives of identity theft crimes and have received TREMENDOUS positive feedback, as they are unable to find this kind of training elsewhere.* Are there any other such training initiatives that the Task Force should consider? *Yes. Many of the crime prevention officers assigned to law enforcement agencies are civilian personnel. These personnel are the ones responsible for educating the consumers and business about identity theft. They should not be excluded from any training that is offered to sworn law enforcement officers. Focus should also be directed to the business community. Because businesses do not receive training on how to detect and prevent fraud at the point of sale, it remains ultimately easy for the criminals to commit the crime. If we can also harden the target at the point of transaction, we also help defeat the crime. If we only focus our efforts on the consumer, that is only half the puzzle. The "big picture" needs to be taken into account.*

8. Measuring Law Enforcement Efforts

Because there is limited data on law enforcement efforts in the area of identity theft, the Task Force is considering whether additional surveys and statistical analysis are needed, including whether to: (a) expand the scope of the National Crime Victimization Survey; (b) review U.S. Sentencing Commission data on identity theft-related case files every two to four years; (c) track federal prosecutions of identity theft and the amount of resources spent on such prosecutions; and (d) conduct targeted surveys in order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police. Would such surveys

be helpful to the law enforcement community? *What purpose would these surveys serve other than to track the incidence of the crime of identity theft? If that is the goal, then yes, they might be useful for tracking statistics. But I don't really see how that is useful to law enforcement to help combat the crime.* Are there any other such surveys or measurements that the Task Force should consider? On a related issue, are the data sets that are currently available that relate to the frequency, cost, and type of identity theft sufficient to give us a full understanding of the problem of identity theft?

Form of Comments

The Task Force requests that interested parties submit written comments on the above questions and/or bring to the attention of the Task Force any additional facts or considerations that would assist in developing a coordinated strategic plan. Comments should be captioned **Identity Theft Task Force** and must be filed on or before Friday, January 19, 2007. Although the Task Force prefers that interested parties file their comments electronically, parties may also submit their comments by mail/hand delivery.

Electronic Filing: If parties choose to submit their comments electronically, they should email the comments to Taskforcecomments@idtheft.gov. The Task Force asks that the email include the parties' contact information and that the substantive comments be attached to the email in Word Perfect, Microsoft Word, or PDF format.

Mail or Hand Delivery: A comment filed in paper form should include "Identity Theft Task Force, P065410," both in the text and on the envelope and should be mailed or delivered to the following address: Federal Trade Commission/Office of the Secretary, Room H-135 (Annex N), 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. Because paper mail in the

Washington, D.C. area and at the FTC is subject to delay, parties should consider submitting their comments in electronic form, as prescribed above. The Task Force requests that any comment filed in paper form be sent by courier or overnight service, if possible.

Lisa Scates

Public Safety Consultant

Published: December 1, 2003 | Updated: September 15, 2006



Lisa Scates has researched, developed, and taught fraud prevention classes and seminars for over seven years in both her private business and via her employment for a municipal government public safety office. She has instructed and consulted for the federal government, corporations, community groups, non-profits, and small businesses. She specializes in counterfeit currency, false identification, credit card fraud, check fraud, and identity theft prevention.

Ms. Scates started her career in the public safety field in 1985 as a Military Police Officer in the United States Army. During her tour in the Republic of Panama, she served 2 years in the undercover contraband and black market unit and 2 years as a patrol officer. After completing her tour of duty she returned to the states and began a nine-year career with the San Marino Police Department.

Since 1999 Ms. Scates has been a senior public safety officer for a local municipality. The curriculum she developed and implemented includes crime prevention classes and seminars covering issues and topics such as identifying credit card/check fraud, detecting counterfeit currency, burglary prevention, robbery protocol, shoplifting prevention, identity theft, senior safety, and personal safety.

Ms. Scates also owns her own public safety consulting business, "GOT FRAUD?", a detection and prevention training solution company that educates merchants and corporations through training their employees how to detect and prevent fraud at the point of sale. GOT FRAUD? additionally works with employers to provide identity theft prevention training to their employees and family members as an added benefit of employment. Besides her many accomplishments, Ms. Scates also serves as a public safety consultant and technical expert for Ready2Protect, LLC and Key Consultants.

During her tenure as a senior public safety officer, she has been recognized for her accomplishments. In May 2001, she was recognized as *Public Safety Practitioner of the Year* and in September of 2001, the California Crime Prevention Officers Association awarded her *Outstanding Crime Prevention Practitioner*. She was also awarded a *Certificate of Special Congressional Recognition* from Congressman Howard McKeon; *Certificate of Recognition* from Senator Pete Knight and Assembly Member George Runner.

Ms. Scates also served as a board member for the California Crime Prevention Officers Association from 2003 to 2005. From 2001 to 2003 Ms. Scates served as a board member for the Antelope Valley Designated Driver Coalition. She has also served as an ambassador for the Palmdale Chamber of Commerce from 2001 to 2005. Since 2004 Ms. Scates has been a panelist on the ROP Law Enforcement Academy Advisory Board. Currently, Ms. Scates is a member of the Organized Retail Theft Committee for the National Association of Property Investigators and a member in good standing with the National Retail Federation and California Crime Prevention Officers Association.

Ms. Scates is certified as a crime prevention practitioner via American River College; as an advanced crime prevention specialist via the American Crime Prevention Institute; in basic Crime Prevention Through Environmental Design (CPTED) via the Los Angeles County Sheriff's Department; in intermediate CPTED via the National Institute of Crime Prevention; and as an advanced CPTED specialist via the American Crime Prevention Institute.