

January 18, 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 Public Comment

Pursuant to the public notice requesting comment on the recommendations of the Identity Theft Task Force, the following is intended to provide policy guidance in several key areas of the Task Force document.

As background, Identity Safeguards has been providing identity theft protection services to individuals and companies since 2003. We have extensive experience in helping organizations prepare for, and respond to, breaches of personally identifiable information. In addition, we have worked closely with law enforcement – both state and federal – over the years to provide information on identity thieves and support active investigations into criminal elements engaged in identity theft. Since the initial purpose of our business was, and continues to be, assisting the victims of identity theft, we have a unique perspective insofar as we see this crime through the eyes of the victim.

I. National Data Security Standards

The Task Force has asked whether national data security requirements should be imposed on all commercial entities that maintain sensitive consumer information. We

believe that any business collecting personally identifiable information, such as a Social Security Number or credit card numbers, has a fiduciary responsibility to safeguard that information. The efficiency of our modern economy requires that commerce happen in real time. As a result, consumers must have faith in the protection of their personal information if growth is to continue in the digital age.

We also understand, however, that not every business has the resources or takes this fiduciary responsibility seriously. They may also have difficulty squaring their good faith efforts with the confusing legal requirements that exist on a state-by-state basis. As such, we support a national standard. But, the standard should be set at the “highest bar” - that is the strongest legal requirement in effect at the state level - rather than the “lowest bar.” The safeguarding of personal information by a commercial entity should be as routine as a business continuity plan. We cannot simply rely on companies to create sound business practices when it comes to personal information. They should be compelled or strongly incentivized to safeguard that information.

1. Essential elements of a national standard – Protection and Response Plan

The essence of a national standard should be the pro-active development and execution of an information safeguards plan to protect consumers’ personal information and an emergency incident plan to respond effectively to a data breach. The protection plan should include safeguards appropriate to the size and complexity of the organization (i.e. security audits, risk mitigation controls, data encryption), privacy and personnel policies to safeguard personal information that exists in hard-copy form, and human resources policies to guard against employees being compromised by criminal elements (i.e. background screening for employees who are responsible for managing personal

data). The emergency incident response plan should include what steps are to occur when there is a data breach event. These steps should include the scope, method and process of notification to potential victims, credit or identity monitoring for that universe, and victim recovery assistance to individuals who fall victim. The plan should be risk-based and adjust for the specific circumstances based on the risk that affected individuals will become victims of identity theft or fraud.

2. *Certification of Plan*

An essential part of ensuring that businesses comply with the creation and implementation of an information safeguards and incident response plan should be written certification – witnessed by a Notary Public - by a Chief Information Officer, or his/her equivalent, that such a plan exists and meets minimum standards (i.e. AICPA recommendations for an incident response). For publicly-traded companies, the plan should be filed with the FTC or SEC but should not be made publicly available. For private companies, the plan should be certified and held at company headquarters. It should be made available to both the FTC and state Attorneys General upon request.

3. *Safe Harbor*

Public and private companies that develop, execute, and certify an information protection and incident response plan should be afforded safe harbor from litigation. We note that there pending court cases that will inform policy makers as to the extent of business liability over the loss of personal information, and the outcome of those cases – particularly at the U.S. Supreme Court level – may define the boundaries of financial responsibility in this area. Nevertheless, strong incentives for businesses to comply with the plan requirements should be offered. Safe harbor should only be provided when it

can be demonstrated that the company was following its protection plan when the breach occurred.

II. Victim Recovery

The law and policy that have been developed around identity theft have been focused on the prevention of the crime through business risk analysis and consumer information and law enforcement tools to track down and prosecute thieves. While the steps taken to date have been very positive and have brought an increasing awareness to the crime, more can be done to help individuals who fall victim. According to recent FTC studies, a victim of identity theft will take 30 to 60 hours of their own personal time and time away from work to bring about a resolution to their case. This is primarily done by somebody utilizing either their own instincts and judgment or an information package (i.e. do it yourself kit) provided by the FTC or other organization. These steps are positive, but the personal and professional time dedicated to resolving the crime is an enormous imposition on an individual and employer, and we find that the case is often re-opened when a thief will try to defraud the identity again. This requires on-going monitoring to detect additional criminal activity and respond to it in real-time.

In order to assist the victim in recovering from identity theft, Identity Safeguards and other organizations have developed a process that utilizes ID Theft Victim Recovery Advocates to work on a one-on-one basis with victims to return them to a pre-identity theft status. Victim assistance should be required for businesses and government agencies that lose data that result in identity theft. This assistance can take the form of credit or identity monitoring and victim restoration services.

1. Victim Recovery Advocate Certification

As more businesses offer services in the area of ID theft victim recovery, we believe that it is important that a minimum set of standards be implemented to ensure the competence of the advocates and effectiveness of the process. Detailed knowledge of federal and state consumer protection law, knowledge of an individual's privacy rights, and a clear understanding of the scope of work that can be provided to a victim are essential if a victim is going to receive an honest and informed package of services in their restoration.

Whether it is Certified Public Accountants, lawyers, credit repair agency representatives or plumbers and electricians, a large number of vital service occupations must pass a certification process in order to be allowed to do business today. We believe that when ID theft Victim Recovery Advocates like those we employ are assisting individuals in the area of identity theft recovery, those individuals should know that the Victim Recovery Advocate has a solid understanding of consumer protection and privacy law. Without minimum standards, we are concerned that businesses will market these services and not be able to adequately assist in the recovery of what is an emotionally-charged and complex crime.

2. Requiring Victim Assistance

While amending the criminal restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in recovering from the crime is a good idea, we don't believe that it will be a meaningful benefit in practice. The most important thing a victim needs at the moment they become victimized is assistance in stopping the thief and restoring their identity. While identity theft has

grown in public awareness, it is still a crime that receives little prosecutorial attention at the state and federal level. Therefore, a victim would have to know his/her thief, trust that they're being prosecuted, and hope that there are assets commensurate with damages in order to be made whole. Then, they'd have to jump through the restitution process in order to receive payment. This is a daunting and, some would say, largely fruitless exercise.

A more meaningful benefit to the individual would be to require that the business that was responsible for the breach that led to their identity theft pay for their recovery. A recent study by ID Analytics shows that 1 in 1,000 of a potential victim pool are actually victimized. As such, the universe and the budget exposure could be contained at a relatively low level versus other solutions (i.e. credit monitoring). We have also seen several data breaches caused by independent contractors employed by businesses to manage a specific process (i.e. audits, loan processing, debt collections). In these cases, the independent contractor was held accountable and paid for the notification and victim assistance for the affected population. Requiring that businesses include data breach protection and indemnification in their contracts with independent contractors will help reduce the incidence of this issue.

3. Identity Monitoring versus Credit Monitoring

Over the course of the last two to three years, credit monitoring has gravitated to the center of the discussion of how to assist victims or potential victims of identity theft who are at risk due to a breach. While this has provided a tangible benefit to the at-risk population, there are two notable shortcomings to credit monitoring as a response. First, credit monitoring simply tells the individual that he/she may have a problem that needs to

be addressed; it does nothing to help support that individual or help them through what can be an altogether daunting restoration process.

Equally as critical, however, is that credit monitoring cannot identify each of the ways in which an individual may be victimized. Other debt instruments, such as debit cards or government assistance programs, are not monitored by the agencies that track credit. Health care identifiers are also at risk since compromised health records have proven to be a target for organized ID theft rings. As identity thieves become more sophisticated and organized they are finding new ways to subvert standardized monitoring products so they can operate outside of the spotlight of tracking systems. New identity theft detection and alert (i.e. monitoring) products are being developed that would allow for the tracking of an individual's identity across a broad range of databases that would more thoroughly track suspicious activity.

If the government is going to codify or promulgate regulations requiring a type of monitoring, we recommend that the language be written broadly enough to allow for new products and technologies that may significantly improve upon the existing credit monitoring products.

III. Breach Notice Requirements – a National Database

We believe that companies should be required to report any data breach to a pre-determined federal agency, like the FTC, and that the information should be made available through a centralized, online web site or national database. This web site or national database of breaches can serve two functions. First, it can eliminate the possibility of fraudulent consumer notification by providing individuals with an independent, 3rd party location they can go to and check the validity of a breach

believe that any business collecting personally identifiable information, such as a Social Security Number or credit card numbers, has a fiduciary responsibility to safeguard that information. The efficiency of our modern economy requires that commerce happen in real time. As a result, consumers must have faith in the protection of their personal information if growth is to continue in the digital age.

We also understand, however, that not every business has the resources or takes this fiduciary responsibility seriously. They may also have difficulty squaring their good faith efforts with the confusing legal requirements that exist on a state-by-state basis. As such, we support a national standard. But, the standard should be set at the “highest bar” - that is the strongest legal requirement in effect at the state level - rather than the “lowest bar.” The safeguarding of personal information by a commercial entity should be as routine as a business continuity plan. We cannot simply rely on companies to create sound business practices when it comes to personal information. They should be compelled or strongly incentivized to safeguard that information.

1. Essential elements of a national standard – Protection and Response Plan

The essence of a national standard should be the pro-active development and execution of an information safeguards plan to protect consumers’ personal information and an emergency incident plan to respond effectively to a data breach. The protection plan should include safeguards appropriate to the size and complexity of the organization (i.e. security audits, risk mitigation controls, data encryption), privacy and personnel policies to safeguard personal information that exists in hard-copy form, and human resources policies to guard against employees being compromised by criminal elements (i.e. background screening for employees who are responsible for managing personal

data). The emergency incident response plan should include what steps are to occur when there is a data breach event. These steps should include the scope, method and process of notification to potential victims, credit or identity monitoring for that universe, and victim recovery assistance to individuals who fall victim. The plan should be risk-based and adjust for the specific circumstances based on the risk that affected individuals will become victims of identity theft or fraud.

2. *Certification of Plan*

An essential part of ensuring that businesses comply with the creation and implementation of an information safeguards and incident response plan should be written certification – witnessed by a Notary Public - by a Chief Information Officer, or his/her equivalent, that such a plan exists and meets minimum standards (i.e. AICPA recommendations for an incident response). For publicly-traded companies, the plan should be filed with the FTC or SEC but should not be made publicly available. For private companies, the plan should be certified and held at company headquarters. It should be made available to both the FTC and state Attorneys General upon request.

3. *Safe Harbor*

Public and private companies that develop, execute, and certify an information protection and incident response plan should be afforded safe harbor from litigation. We note that there pending court cases that will inform policy makers as to the extent of business liability over the loss of personal information, and the outcome of those cases – particularly at the U.S. Supreme Court level – may define the boundaries of financial responsibility in this area. Nevertheless, strong incentives for businesses to comply with the plan requirements should be offered. Safe harbor should only be provided when it

can be demonstrated that the company was following its protection plan when the breach occurred.

II. Victim Recovery

The law and policy that have been developed around identity theft have been focused on the prevention of the crime through business risk analysis and consumer information and law enforcement tools to track down and prosecute thieves. While the steps taken to date have been very positive and have brought an increasing awareness to the crime, more can be done to help individuals who fall victim. According to recent FTC studies, a victim of identity theft will take 30 to 60 hours of their own personal time and time away from work to bring about a resolution to their case. This is primarily done by somebody utilizing either their own instincts and judgment or an information package (i.e. do it yourself kit) provided by the FTC or other organization. These steps are positive, but the personal and professional time dedicated to resolving the crime is an enormous imposition on an individual and employer, and we find that the case is often re-opened when a thief will try to defraud the identity again. This requires on-going monitoring to detect additional criminal activity and respond to it in real-time.

In order to assist the victim in recovering from identity theft, Identity Safeguards and other organizations have developed a process that utilizes ID Theft Victim Recovery Advocates to work on a one-on-one basis with victims to return them to a pre-identity theft status. Victim assistance should be required for businesses and government agencies that lose data that result in identity theft. This assistance can take the form of credit or identity monitoring and victim restoration services.

1. Victim Recovery Advocate Certification

As more businesses offer services in the area of ID theft victim recovery, we believe that it is important that a minimum set of standards be implemented to ensure the competence of the advocates and effectiveness of the process. Detailed knowledge of federal and state consumer protection law, knowledge of an individual's privacy rights, and a clear understanding of the scope of work that can be provided to a victim are essential if a victim is going to receive an honest and informed package of services in their restoration.

Whether it is Certified Public Accountants, lawyers, credit repair agency representatives or plumbers and electricians, a large number of vital service occupations must pass a certification process in order to be allowed to do business today. We believe that when ID theft Victim Recovery Advocates like those we employ are assisting individuals in the area of identity theft recovery, those individuals should know that the Victim Recovery Advocate has a solid understanding of consumer protection and privacy law. Without minimum standards, we are concerned that businesses will market these services and not be able to adequately assist in the recovery of what is an emotionally-charged and complex crime.

2. Requiring Victim Assistance

While amending the criminal restitution laws to allow identity theft victims to seek restitution from the identity thief for the value of their time in recovering from the crime is a good idea, we don't believe that it will be a meaningful benefit in practice. The most important thing a victim needs at the moment they become victimized is assistance in stopping the thief and restoring their identity. While identity theft has

grown in public awareness, it is still a crime that receives little prosecutorial attention at the state and federal level. Therefore, a victim would have to know his/her thief, trust that they're being prosecuted, and hope that there are assets commensurate with damages in order to be made whole. Then, they'd have to jump through the restitution process in order to receive payment. This is a daunting and, some would say, largely fruitless exercise.

A more meaningful benefit to the individual would be to require that the business that was responsible for the breach that led to their identity theft pay for their recovery. A recent study by ID Analytics shows that 1 in 1,000 of a potential victim pool are actually victimized. As such, the universe and the budget exposure could be contained at a relatively low level versus other solutions (i.e. credit monitoring). We have also seen several data breaches caused by independent contractors employed by businesses to manage a specific process (i.e. audits, loan processing, debt collections). In these cases, the independent contractor was held accountable and paid for the notification and victim assistance for the affected population. Requiring that businesses include data breach protection and indemnification in their contracts with independent contractors will help reduce the incidence of this issue.

3. Identity Monitoring versus Credit Monitoring

Over the course of the last two to three years, credit monitoring has gravitated to the center of the discussion of how to assist victims or potential victims of identity theft who are at risk due to a breach. While this has provided a tangible benefit to the at-risk population, there are two notable shortcomings to credit monitoring as a response. First, credit monitoring simply tells the individual that he/she may have a problem that needs to

be addressed; it does nothing to help support that individual or help them through what can be an altogether daunting restoration process.

Equally as critical, however, is that credit monitoring cannot identify each of the ways in which an individual may be victimized. Other debt instruments, such as debit cards or government assistance programs, are not monitored by the agencies that track credit. Health care identifiers are also at risk since compromised health records have proven to be a target for organized ID theft rings. As identity thieves become more sophisticated and organized they are finding new ways to subvert standardized monitoring products so they can operate outside of the spotlight of tracking systems. New identity theft detection and alert (i.e. monitoring) products are being developed that would allow for the tracking of an individual's identity across a broad range of databases that would more thoroughly track suspicious activity.

If the government is going to codify or promulgate regulations requiring a type of monitoring, we recommend that the language be written broadly enough to allow for new products and technologies that may significantly improve upon the existing credit monitoring products.

III. Breach Notice Requirements – a National Database

We believe that companies should be required to report any data breach to a pre-determined federal agency, like the FTC, and that the information should be made available through a centralized, online web site or national database. This web site or national database of breaches can serve two functions. First, it can eliminate the possibility of fraudulent consumer notification by providing individuals with an independent, 3rd party location they can go to and check the validity of a breach

notification. Second, it can provide a powerful incentive for businesses to implement effective protection plans. Businesses who do not want to be listed on a national registry of companies that have experienced breaches will be more diligent about ensuring the protection of the personal information in their possession.

The reporting requirement and the public listing of the breach should not discriminate between ownership type, size, or sector of the business. The information provided should include the name of the business, the date of the breach, the type of data stolen (soft or hard data, SSN, health records, etc.), the actual or perceived location of the breach event, the size of the at-risk pool, and a contact number or website where potential victims can seek additional information.

IV. Law Enforcement

IDS has developed a close working relationship with law enforcement from both the state and federal levels as we've warehoused a considerable amount of information on identity thieves and criminal organizations. It's been clear to us that law enforcement faces a major lack of resources to train properly in matters pertaining to data breaches and personal information. The lack of resources means the thieves always have better equipment and law enforcement will typically lag behind the training necessary to combat the problem.

Additionally, when states are enacting legislation a continuing pattern is uncertainty about enforcement and penalties. Where will the enforcement reside when new programs and procedures are legislated? Many states cannot use the general fund to fund and implement these pieces so they simply go un-enforced. The best laws cannot be effective without an agency to enforce them.

notification. Second, it can provide a powerful incentive for businesses to implement effective protection plans. Businesses who do not want to be listed on a national registry of companies that have experienced breaches will be more diligent about ensuring the protection of the personal information in their possession.

The reporting requirement and the public listing of the breach should not discriminate between ownership type, size, or sector of the business. The information provided should include the name of the business, the date of the breach, the type of data stolen (soft or hard data, SSN, health records, etc.), the actual or perceived location of the breach event, the size of the at-risk pool, and a contact number or website where potential victims can seek additional information.

IV. Law Enforcement

IDS has developed a close working relationship with law enforcement from both the state and federal levels as we've warehoused a considerable amount of information on identity thieves and criminal organizations. It's been clear to us that law enforcement faces a major lack of resources to train properly in matters pertaining to data breaches and personal information. The lack of resources means the thieves always have better equipment and law enforcement will typically lag behind the training necessary to combat the problem.

Additionally, when states are enacting legislation a continuing pattern is uncertainty about enforcement and penalties. Where will the enforcement reside when new programs and procedures are legislated? Many states cannot use the general fund to fund and implement these pieces so they simply go un-enforced. The best laws cannot be effective without an agency to enforce them.

A major argument from business is that law enforcement needs to be the governing body when there is a breach of personally identifiable information. Aside from responding and investigating to the breach, law enforcement is admittedly ill-equipped to handle many of the additional burdens aimed at the victims. Who, for instance, is the outside and unbiased third-party who will verify an affected population “risk” to ID theft in cases where notification is optional? Is it law enforcement? We think that it an overly burdensome requirement.

We recommend Departments like the Department of Consumer and Business Services in Oregon head the efforts collaboratively with their Attorneys General, law enforcement, and private firms specializing in ID theft restoration, victim advocacy, and breach law compliancy. Penalties should be stiff to set precedents that negligent treatment of consumer personal information will not be tolerated. And, as noted in the above “victim assistance” discussion, businesses that are liable for the data breach should be required to notify and assist victims who are compromised by the loss of data entrusted to that business. Law enforcement should focus on investigating and prosecuting the perpetrator so they cannot claim any additional victims.

Conclusion

Identity Safeguards has developed a broad expertise in the area of identity theft. Most importantly, however, we have worked directly with victims and understand the emotional and financial hardship they experience while dealing with this most personal of crimes. Every level of government has a role in informing the public about the dangers of personal data being compromised and tracking down criminals who trade on our good names.

We believe also that the private sector has a responsibility to safeguard our information and that they should be compelled to do so. If the information we give them in exchange for our business is compromised, those businesses should share in the response and resolution to that breach. That is a fiduciary responsibility they owe to their customers.

Sincerely,

Rick Kam

President