STATEMENT

OF

CATHERINE A. ALLEN

CHAIRMAN AND CEO, THE SANTA FE GROUP

INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES SUBCOMMITTEE

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE

"IDENTITY THEFT: A VICTIMS BILL OF RIGHTS"

WEDNESDAY, JUNE 17, 2009

2154 Rayburn HOB

2:00 p.m.

Testimony of Catherine A. Allen
Chairman and CEO, The Santa Fe Group

June 17, 2009

Introduction

Chairman Clay, Ranking Member McHenry, and members of the Subcommittee, thank you for your leadership in highlighting the issue of victims of identity crime — especially those who are victims of the most complex and invasive of these crimes — and the often long and lonely road they walk toward restoration.

I am Catherine Allen, Chairman and CEO of The Santa Fe Group, a strategic consulting firm specializing in emerging technologies, risk management, payments strategies, innovation and public policy. The Santa Fe Group is based in Santa Fe, New Mexico, and serves global clients.

I have spent most of my career in the financial services industry. From 1996 to 2007, I was the Founding CEO of BITS, a CEO-driven nonprofit financial services industry consortium and think tank, focused on emerging technologies, fraud prevention, cybersecurity, and payments. Its members are 100 of the largest financial institutions in the US. BITS is now a division of The Financial Services Roundtable.

Today I am also involved in efforts to examine the way the financial services industry is regulated and the impact of industry policy on consumers. These efforts include advisory roles in the Bipartisan Policy Center's Regulatory Reform Roundtables and the Financial Services Regulatory Reform Collaborative. I also chair the advisory board of the National Foundation for Credit Counseling. In each of these roles, I work to explore the interaction of the financial services industry with consumer, economic, and regulatory issues facing our country and the global community.

Today's testimony reflects the work of The Santa Fe Group Vendor Council, which was formed in 2006 to bring together thought leaders at service provider organizations to respond to the needs of industry, including financial services, government, and regulatory agencies, and other constituents, and to encourage innovative, forward-thinking strategies that benefit all of us. The Vendor Council promotes the development of secure, best-in-class technology solutions, standards, and business processes, as well as industry best practices related to fraud, payments, cybersecurity, data protection, and identity crime.

Last fall, the Vendor Council formed an Identity Management Working Group to develop an inventory of best practices for assisting victims of identity crime and suggesting improvements in law and corporate practice to make it easier for victims to dispute false records and reclaim their identity. A first step was the release of a draft briefing paper entitled *Victims' Rights: Fighting Identity Crime on the Front Lines* in April of this year. The Vendor Council continues to work on this issue.

Like you, Chairman Clay, I am originally from Missouri. In April I spoke to more than 300 Missourians about identity crime at the University of Missouri along with Rick Kam, Chair of the Vendor Council's Identity Management Working Group and President of member company, ID Experts.

While the Internet has brought tremendous local and global opportunities, the proliferation of its use by criminals has endangered ordinary Americans in new ways. I'm speaking in particular about the financial health and privacy of the average American.

Identity crime is a global economic problem. It is a low-overhead, high-margin business for criminals and can be performed from a distant location; indeed, not just across a state or a country, but from another continent. Identity theft can also be perpetrated right in your own back yard, from "dumpster diving" to mail theft, to people who prey on unsuspecting relatives with whom they share a home. The reason I focus in part on data breaches today is that identity theft is increasingly perpetrated on a large scale by sophisticated organized criminals around the globe who no longer have to risk bodily harm to perpetrate their crime. They just need a computer and a sophisticated understanding of information technology systems. Crimes targeting ordinary Americans originate in the Ukraine, Nigeria, and other far-flung locations around the globe. And I believe what we're seeing now is just the tip of the iceberg.

Millions of dollars are being poured into efforts to halt identity theft. This is appropriate. That said, I believe that the discussion of identity theft too often leaves one important voice out of the debate: the victim. It is on behalf of victims' rights that I come to testify before you today.

Identity crime losses are expected to grow exponentially as more and more crimes put victims in the middle of large-scale cybersecurity attacks. Many of these attacks will not be discovered for years, placing the victims in the most vulnerable position. When I last testified before you on one panel, the CIO of the State of Missouri talked about the theft of student information from the University of Missouri's law and medical schools. The criminals, who were apprehended, said they planned to hold the information for ten years, and then use it to perpetrate identity crime against those students, who by then were likely to have significant assets.

The Victim Experience

Victims of true identity crime, which goes far beyond theft and one-time use of a credit or debit card, often suffer financially and may bear a significant burden in time spent recovering. Various studies put the expense to victims at anywhere from $0 to $950 and the time spent at anywhere from four to 165 hours. Many victims have their credit card applications denied or their existing accounts canceled; others are denied loans or lines of credit. Children's identities are stolen before they're old enough to write their own names, leaving parents to sort out the problem and clean up their records. Given the state of the

economy, this all adds up to a tremendous hardship at a time when individuals and families are already suffering. Indeed, low-income families in particular suffer when identity crime strikes.

In spite of consumer protection laws, identity crime victims, especially those who are victims of complex and invasive forms of identity crime, are often thwarted in recovering and restoring their own identities. Many victims face a complex and disjointed maze, however well-intended, of privacy laws, public and private information sources, and financial, law enforcement and other organizations, each with distinct rules and priorities. As a result, a victim's life can be disrupted for years. In addition to financial losses from identity crime, businesses experience lost productivity and consumer distrust. In cases of medical identity theft, misinformation may become part of a person's medical record, potentially endangering their health and well-being and the integrity of our electronic healthcare system in general.

Our focus on victims' rights is an attempt to bring awareness to the plight of individuals whose information is stolen for the express purpose of identity theft. Too often identity crime is treated as victimless, which it is certainly not.

Although legislative and law enforcement responses to identity crime are evolving, victims still lack adequate protection and support, with at times devastating effects. Here are just a few examples of the challenges and frustrations experienced by some identity crime victims:

- The victim may not realize a crime has occurred for months or even years, by which time his or her financial, medical, and civil identities may all have been damaged. A report by the Economic Crime Institute of Utica College and LexisNexis found that 20% of identity theft resulted in multiple crimes.

- The victim may have to deal with a confusing array of businesses and institutions. To help correct records, victims may request written documentation of identity misuse, but financial, medical, or other organizations sometimes refuse on the basis of current privacy laws that protect data but do not necessarily permit access to data, or they may insist on being provided proof from law enforcement or some other organization that a crime has occurred.

- Some states now have legal requirements that victims file a police report. (Victims' rights groups have advocated for these laws to help real victims while preventing fraudsters and pretexters from using false claims to access sensitive information for improper purposes.) But law enforcement processes are not always in place, so when victims try to file a report with police, they may be told that they don't need to file a report or that they need to talk to one or more additional departments. And many individual identity crimes fall below the financial threshold that would trigger federal, state, or even local law enforcement agencies to act. Unfortunately, this permits large organized crime identity theft scams to go undetected for months and years, adding one individual identity theft victim after another.

- Law enforcement may not prosecute identity theft crimes. And even if convinced that transactions are fraudulent, some businesses won't pursue or prosecute thieves when it doesn't make financial sense to do so.

- In some cases, victims are suspected of claiming identity theft to avoid paying legitimate charges. Victims may be required to establish that a crime has occurred. When victims are already in debt, some financial institutions may be predisposed to accuse them of scamming.

- Many organizations won't share evidence with victims. A victim may not be allowed to see applications submitted in his or her name, even though these documents could help the victim locate and stop the identity thief. Access to data held about an individual is one of the global privacy principles that has not yet been implemented into US laws as it has in other countries.

- Privacy laws make medical identity theft even harder to combat. Medical institutions are required by the Health Insurance Portability and Accountability Act (HIPAA) to protect patient information, and some organizations believe that applies even if that patient is being treated under a false identity, making it very difficult for victims to remove misinformation from their medical records. The Department of Health and Human Services (HHS) is attempting to educate the medical community that HIPPA does not intend to restrict patients from changing false data.

- If criminal acts are committed under a stolen identity, the first news a victim often has of the theft may be when he or she is arrested. And if a person is falsely arrested or if a pre-employment background check incorrectly indicates a criminal record, the victim may need to go through a "reverse booking," which requires the person to prove his or her innocence.

In addition to these obstacles, there are significant non-monetary effects on identity crime victims when the crimes are complex, just as there are in violent crimes. Victims often receive little emotional support from family, friends, colleagues, and employers who don't understand the challenges of identity recovery. According to a 2008 report by the Identity Theft Resource Center, identity crime victims that responded to their survey expressed feelings of rage, anger, and betrayal; the sense that they were powerless; personal financial fears; and feelings of loss of innocence. They also reported sleep disturbances and an inability to trust other people. Long-term emotional responses included suicidal thoughts (4%), the desire to give up and stop fighting the system (25%), and the feeling that they had lost everything (10%).

Public and Private Sector Efforts to Help Victims

A number of government and industry organizations deal with identity crime in some capacity. These efforts represent substantial steps in responding to identity crime and assisting victims.

The Federal Trade Commission (FTC) is the center of public outreach efforts, providing consumers with information on identity theft scams, steps to take if you think you're a victim, a recovery toolkit, and other resources through its website and support center. The website offers comprehensive identity crime information, from a quiz for consumers to gauge their identity crime knowledge to in-depth reports, guides for businesses and information about the President's Identity Theft Task Force. In addition, the FTC has made recommendations to Congress on limiting the use and display of Social Security numbers, provided training to law enforcement and others who can assist identity theft victims, and enforced new identity-theft related rights under the Fair and Accurate Transactions Act, such as the right to free annual credit reports.

The Department of Justice (DOJ) prosecutes identity crimes, working with the FBI, US Secret Service and the US Postal Inspection Service. Its website offers information for consumers about identity crime, including what to do if you think you may be a victim. The DOJ is part of the Interagency Working Group on identity theft and works with the FTC and other agencies that have a stake in identity crime.

The Social Security Administration (SSA) presents an electronic fact sheet for consumers and works with the FTC and other government agencies to prosecute identity crime involving Social Security. The agency also provides some victim services such as replacement of lost or stolen Social Security cards, corrections to earnings records and, in special circumstances, issuance of a new Social Security number.

In addition to these government agencies, there are several private-sector organizations aimed at helping consumers. The Identity Theft Resource Center (ITRC), which is also giving testimony today, is a private not-for-profit that conducts research; advises policymakers, law enforcement and businesses; and provides consumer and victim support as well as public education.

The Identity Theft Assistance Center (ITAC) was created in 2004 by 50 of the nation's largest financial services companies under the sponsorship of BITS and The Financial Services Roundtable. Today the ITAC provides free victim assistance and has helped more than 55,000 consumers restore their financial identity.

The Privacy Rights Clearinghouse is a nonprofit consumer education and advocacy project that advocates for consumers' privacy rights in public policy proceedings, and the Electronic Privacy Information Center (EPIC) is a public interest research center established "to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."

While all of these efforts are meaningful and do help, much more can and should be done to help victims.

The Legislative Landscape

Lawmakers have been aware of identity theft since the late 1990s. There are several federal laws related to identity crime. There are also hundreds of state laws on identity crime that vary widely in their approach.

Federal legislation on identity crime includes:

Identity Theft Enforcement and Restitution Act of 2008
This legislation makes it easier to bring hacking and other cybercrime charges against an individual, eliminating the federal requirement that prosecutors show the crime caused at least $5,000 in damages. In addition, this law makes it possible to bring felony charges against multiple offenders, allows crimes committed within a single state to be prosecuted in federal courts, and directs the U.S. Sentencing Commission to review its guidelines and consider increasing the penalties for those convicted of identity theft, computer fraud, illegal wiretapping, or breaking into computer systems.

GLBA and Financial Services
The Gramm-Leach-Bliley Act (GLBA), aimed at the financial services industry, provides significant privacy protections against the disclosure of nonpublic personal information. GLBA includes safeguards such as: certain data, such as account numbers, cannot be used for marketing under any circumstances; nonpublic personal information may not be disclosed unless consumers are given notice of information-sharing policies and the opportunity to opt-out of information-sharing activities; and financial service providers are required to employ data security safeguards to protect personal information. Financial institutions are also required to provide notice of data breaches.

HIPAA and Medical Privacy
Enacted to protect health insurance coverage for workers and their families when they change or lose their jobs, the Privacy Rule of HIPAA establishes regulations for the use and disclosure of Protected Health Information (PHI), which includes any information about health status, provision of healthcare, or payment for healthcare that can be linked to an individual. In practice, PHI is taken to include any part of a patient's medical record or payment history. Congress recently enacted legislation requiring entities that maintain PHI to notify individuals in case of a breach. The FTC and HHS are currently promulgating their own rules to implement this requirement.

FACTA and the Red Flag Rule
The Fair and Accurate Credit Transaction Act of 2003 (FACTA) added new sections to the Fair Credit Reporting Act (FCRA) granting consumers the right to free credit reports, the right to place fraud alerts on credit accounts, and the right to obtain copies of fraudulent documents and to obtain debt information from collections agencies. FACTA also allows

consumers a right to an Identity Theft Report that can empower the consumer to block the reporting of fraudulent data by credit reporting agencies and data furnishers; it can also be used to require collection agency activity to stop. Under the terms of the Red Flag Rule of FACTA, all financial institutions and creditors will be required to have a program in place to prevent and mitigate the effects of identity theft. The FTC has published guidelines on recognizing identity theft and established 26 red flags that financial institutions should consider when creating their mandatory identity theft programs.

Government Requirements on Data Breach
According to a memorandum issued February 4, 2008, from the U.S. Office of Management and Budget: "In the event of a data breach, government agencies [must] promptly conduct a risk analysis and be prepared to submit a report containing the findings to the Congressional Oversight Committees of the U.S. Senate and House of Representatives, as appropriate." As indicated, government data breach policies focus on assessment with an occasional nod towards victim notification and credit protection. Faced with limited resources, government agencies are focused mainly on preventing large-scale data breach incidents.

Additionally, the Privacy Act of 1974, which focused on government acquisition of data on US citizens, established a penalty for data breaches and the right of individuals to request release of their information.

REAL ID Act
Under the Real ID Act, states are encouraged to implement more secure drivers' licenses. In conformance with federal requirements, states are instituting more secure forms of personal identity (driver's licenses, etc.). Many now require additional "breeder documents" to establish identity (such as passports and certified birth certificates), and they use secure manufacturing processes and incorporate watermarking, holograms, or other advanced security features into the documents.

State Laws on Identity Crime
Currently, 44 states have laws requiring that an organization notify every person whose privacy was compromised when customer or employee data is lost or leaked. (Generally these apply to unencrypted personal information.) While the requirements vary by industry and jurisdiction, failure to notify will put most organizations at risk of legal and financial penalties. Some states are also issuing "identity passports" to identity theft victims, certifying that their identity has been stolen, and helping protect them from false arrest and other risks. How effective these documents are remains to be seen. A number of states have taken steps to implement information security laws, notably Massachusetts, where all types of organizations — not only financial institutions — that process personal information on Massachusetts residents will be required to have a comprehensive information security program in place beginning January 1, 2010. This program was created to meet a number of prescriptive requirements.

A number of bills are pending right now that would be appropriate vehicles for victims' rights provisions. We look forward to providing our expertise at the appropriate time to

ensure upcoming legislation includes language that protects the rights of identity crime victims.

An Identity Crime Victims Bill of Rights

Identity crime victims deserve the same rights as other crime victims. Identity crimes can have physical, emotional, and financial impacts comparable to other crimes. While much is being done in the private and public sectors to help victims, we still lack adequate provisions for restoration, reparation, or even prosecution. Today, most identity crimes will be treated as misdemeanors or very low-level felonies, and the majority of prosecutions will be civil as opposed to criminal actions for both individuals and organized crime thefts. We need better coordination, awareness of the victim experience, and concrete steps for correcting identity records.

For the benefit of individuals, business, and society, I propose the following rights for identity crime victims:

- The right to assessment
- The right to restoration
- The right to freedom from harassment
- The right to potential prosecution of the offender(s)
- The right to restitution

Below are some concrete steps that policymakers can take towards empowering victims to stem the tide of identity crime.

Right to Assessment
Consumers who suspect they have become a victim of identity crime should have the right to assess the nature and extent of damage to their identity. FACTA already grants many of these rights, but consumers face procedural Catch-22s when trying to exercise them. For example, consumers often must present a bank with a police report before they can retrieve the information needed to assess their situation, but most police departments won't take a report without evidence of a crime. (The policing community, including the International Association of Chiefs of Police, has increasingly recognized the need to take such reports, and more police departments around the country are doing so.) Businesses and law enforcement need effective, uniform requirements and processes for handling identity theft cases, and relevant privacy laws must be reviewed and amended to protect identity crime victims instead of thwarting their recovery.

Businesses and government agencies should be required to provide notice to consumers when they suffer a data breach involving loss of sensitive personal information. The present patchwork of state laws and government policy needs to be replaced with a uniform federal statute spelling out notification requirements. Clear guidelines would help businesses contain costs and limit legal liability through compliance and enhance

consumer protection. Any federal law should contain a "safe harbor" provision for small businesses, setting their notification requirements at an affordable level with scalable data security safeguard requirements.

Right to Restoration
Ideally, victims should be able to restore their identities to their pre-theft state. However this is not always possible because of the complexity of the crime, especially in cases of financial identity theft. Whether or not they can fully recover, it is imperative that victims be able to establish correct records. Relevant privacy laws need to be reviewed and amended, giving victims the power to access and correct their own record in cases of identity crime. One issue up for debate is how to provide the right of consumer access and correction without jeopardizing the integrity and reliability of the underlying records. To empower consumers and ease companies' fears about liability, lawmakers and industry could charter an organizational entity that operates across the public and private sectors and validates identity, just as credit bureaus and Public Key Infrastructures perform similar services around identity today. This model could be tested initially as a private service, but it ultimately needs to be publicly available.

As with the right to assessment, identity restoration would be far simpler if we could do away with the patchwork of state laws and create one federal standard. Businesses support this notion, because it will limit their liability, simplify processes, and mitigate costs.

Right to Freedom from Harassment
Identity crime victims should be protected from harassment by collection agencies and others during and after the identity restoration process. Harassment often continues unabated because business and law enforcement have no way to distinguish victims from debtors and thieves. To combat this some states are issuing identity theft "passports" to verify that the carrier has been a victim of identity theft and help the person prove his or her identity. How effective these documents are remains to be seen. (The DOJ's Office for Victims of Crime funded the Ohio Attorney General's identity theft passport program as a demonstration program, but the department has not yet fully evaluated the program's effectiveness.) In any case, victims desperately need a reliable way to identify themselves and prove they are who they say they are.

Right to Potential Prosecution of Offenders
One of the great frustrations to identity crime victims is the lack of business and law enforcement resources to prosecute identity thieves. Of course, law enforcement needs to balance priorities and budgets, and business must weigh the costs and benefits of prosecution. However, these organizations need to also take the long view on the impact of identity crimes:

- First, identity crime continues precisely because it pays. If prosecution stops the payoff, it will help to deter the crime and contain future costs.
- Second, the FBI and Secret Service have found that where there is one victim, there are more. So instead of writing off the costs of an individual case, organizations

should consider that for every instance of identity crime, there may be many others as yet undiscovered or yet to be committed by the same crime ring or individual.
- Third, not all the costs of identity crime are immediately visible or measurable. This fact needs to be taken into account when weighing the costs of prosecution. There should also be increasing accountability for businesses that fail to reasonably secure personal information. Today many states and certain industries have notification requirements for data breach. Other states are taking steps to implement information security laws, and certain sectors (healthcare and financial) have safeguards rules in place.

Right to Restitution
Identity crime victims can spend hundreds of dollars and dozens of hours, and can experience untold misery during the process of restoration. They deserve restitution, the same as victims of other crimes, yet a study by the Center for Identity Management and Information Protection shows that defendants were ordered to pay restitution in only about a third of the cases studied. Restitution will help make victims whole, sends a message that identity crime is real crime, and helps ensure that when perpetrators are caught, identity crime does not pay.

The need for restitution has begun to be addressed at the national level through the Identity Theft Enforcement and Restitution Act of 2008, which makes it easier for victims to claim compensation from convicted offenders. The law states that in cases where convicted identity thieves are ordered to pay restitution, the victim should get a portion of the money "equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offense." Compensation for time is only a start, but it is a good start. To further help victims, the definition of "compensable crime" under federal and state statutes should be expanded to include identity crimes. Finally, the Department of Justice has specific statutory obligations with respect to crime victims, including restitution. However, in many cases full restitution is effectively impossible where the cost to the victim substantially exceeds a convicted offender's financial resources.

Recommendations for Protecting Victims' Rights

In summary, my testimony today advocates for the following legislative actions to help victims:

- **Do away with the patchwork of state laws for identity restoration and create one federal standard.**
- **Require a federal standard for mandatory law enforcement breach reporting for all sectors and cost-effective breach notification to consumers.**
- **Enact a uniform scheme across industry and government to assist identity theft victims: include assessment, rectification, freedom from harassment, authentication, and protection of information for victims.**

- **Create a national standard of identification — one that cannot be forged by identity thieves — that victims can use to distinguish themselves from thieves and identify themselves to businesses, law enforcement and others.**
- **Expand the definition of "compensable crime" under federal and state law to include identity crime.**

Additionally, these steps could be taken right now to strengthen victims' rights and help stem the tide of identity theft:

1. Invest in independent research on the effects of identity crime. To make fully informed decisions, we need a thorough understanding of the costs of identity crime. We aren't prepared to create comprehensive, effective solutions because there are too many unanswered questions about what's happening in policy, industry, and law enforcement. Organizations should be tracking the costs of identity theft, and there should be public funding available to assess the effectiveness and effects of policy, either built into legislation or in the budgets of organizations such as the Department of Justice and FTC. Independent research could lead to improved practices, better education, evidence-based policy, and better ways to authenticate people's identities when conducting public or private transactions.

2. Create standard dispute procedures in industry and law enforcement. Upon resolution, victims would receive standardized, verifiable letters proving that issues had been resolved.

3. Empower the FTC to oversee victims' rights. The FTC should be charged with oversight of proposed policies for cohesion across national laws for effectiveness, and to anticipate and prevent unexpected consequences. This should include ensuring that law enforcement is investigating identity crime cases consistently and effectively. This approach would work in concert with the efforts of programs such as the Social Security Administration, the Pentagon and Veterans Administration, Homeland Security, Medicare, and others to create consistent policies and processes regarding identity theft.

4. Include identity theft victims' rights in any dialogue about a Financial Product Safety Commission. If a proposed commission focused on financial products and services emerges, financial identity theft policies and education might be considered under its jurisdiction and should be included in the dialogue.

Conclusion

Mr. Chairman, many victims of identity crime suffer greatly in the aftermath of this crime. They continue to receive constant reminders of the crime as new information surfaces about the misappropriation of their identity. To make matters worse, policy and protocols often fail to meet their recovery needs.

Establishing a Victims Bill of Rights and including it in consumer protection legislation is a fundamental first step in achieving awareness, consensus and the collaboration required to develop practical solutions.

Thank you for this opportunity to present on the plight of victims and the Victims Bill of Rights, and thank you, again, for your leadership in bringing light to this important issue. Our group stands as a ready resource to you and the other members of this committee as you consider ways to protect and support victims of identity crime.