



American Prosecutors  
Research Institute

# *Who's on First?*

Challenges Facing Prosecutors  
and Financial Institutions in  
Responding to Identity Theft



**National District Attorneys Association  
American Prosecutors Research Institute**

99 Canal Center Plaza, Suite 510  
Alexandria, VA 22314  
[www.ndaa.org](http://www.ndaa.org)

**Thomas J. Charron**  
President

**Roger Floren**  
Chief of Staff

**M. Elaine Nugent-Borakove**  
Director, Office of Research and Evaluation

**David LaBahn**  
Director, NDAA Research and Development Division

This information is offered for educational purposes and is not legal advice. This document was produced under Award No 2005-MU-BX-K046 from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions expressed are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice, the National District Attorneys Association, or the American Prosecutors Research Institute.

2007 by the American Prosecutors Research Institute, the research and development division of the National District Attorneys Association.

The FIRST DATA name and logo is a registered service mark of First Data Corporation. The STAR name and logo is a registered service mark of Star Systems, Inc. These marks are used with permission from their respective owners.

---



National District Attorneys Association  
American Prosecutors Research Institute  
99 Canal Center Plaza, Suite 510  
Alexandria, Virginia 22314  
Phone: (703) 549-9222  
Fax: (703) 836-3195  
<http://www.ndaa.org>

---

# *Who's on First?*

## Challenges Facing Prosecutors and Financial Institutions in Responding to Identity Theft

*June 2007*

*Lisa M. Budzilowicz  
M. Elaine Nugent-Borakove*



# TABLE OF CONTENTS

<b>1</b>	<b>Acknowledgements</b>
<b>3</b>	<b>Introduction</b>
<b>7</b>	<b>Challenges Facing Prosecutors and Financial Institutions</b>
<b>7</b>	<i>Determining What Constitutes Identity Theft</i>
<b>8</b>	<i>Reporting Identity Theft</i>
<b>11</b>	<i>Establishing Points of Contact</i>
<b>12</b>	<i>Barriers to Information Sharing</i>
<b>15</b>	<i>Resources for Investigating and Prosecuting Identity Theft</i>
<b>16</b>	<i>Victims' Issues</i>
<b>19</b>	<b>Strategies for Overcoming Barriers to Cooperation</b>
<b>19</b>	<i>Build Partnerships, Task Forces, and Collaborative Relationships to Share Knowledge</i>
<b>22</b>	<i>Develop Mutual Understanding of Information Needs and Restrictions through Cross-Training</i>
<b>23</b>	<i>Educate Constituent Groups</i>
<b>25</b>	<b>Conclusion</b>
<b>27</b>	<b>References</b>
<b>29</b>	<b>Appendix A: Methodology</b>
<b>31</b>	<b>Appendix B: Contacts and Resources</b>
<b>31</b>	<i>Federal Agencies</i>
<b>34</b>	<i>Federal Laws</i>
<b>35</b>	<i>Task Forces</i>
<b>46</b>	<i>State Government Resources</i>
<b>46</b>	<i>Associations and Non-Governmental Organizations</i>
<b>52</b>	<i>Other Links and Resources</i>
<b>55</b>	<b>Appendix C: Contact Information for Symposium Members</b>



# ACKNOWLEDGEMENTS

The National District Attorneys Association and American Prosecutors Research Institute would like to acknowledge the contributions of numerous individuals who aided in the preparation of this publication and without whose commitment and support this document would not be possible.

Kathryn Keefer, Director of Strategic Marketing at First Data and Barbara Span, Vice President of Public Affairs at Western Union for their dedication and guidance on the project, and for soliciting the vital participation of financial institutions.

All the prosecutors, law enforcement representatives, victims' organizations, financial institutions, and representatives of the U.S. Department of Justice who volunteered their time to serve as members of the advisory group and who provided valuable input for the publication, especially Susan Storey, Senior Deputy Prosecuting Attorney, King County Prosecuting Attorney's Office.

The many prosecutors' offices and financial institutions nationwide that provided their knowledge and experiences with regard to identity theft.

Finally, we would like to thank our federal project officers Michelle Shaw, Kim Norris, and Dara Schulman, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice for their ongoing interest, support, and continuous commitment to the development of such a resource for prosecutors and financial institutions.



# INTRODUCTION

**F**raud, as a crime, is hardly a new concept. Yet in the twenty-first century, methods of committing fraud are more diverse and sophisticated. According to the Federal Trade Commission (FTC), identity theft complaints have accounted for more than one-third of all fraud complaints from 2004 through 2006 (Federal Trade Commission, 2007). There is clearly a growing recognition of the dangers posed by identity theft, yet prosecutors and financial institutions face a number of challenges in formulating comprehensive responses—particularly related to collaborating on the investigation and prosecution of identity theft cases. All too often, these challenges become much like the familiar Abbott and Costello routine: “Who’s on first?” “What’s on second?” “I don’t know is on third.” Who should take the lead? What are each party’s responsibilities? Finally, what do you do when you just don’t know what to do? The solutions to these questions are not necessarily straightforward or easy, and may not be relevant or applicable in all states or at all financial institutions. However, examining how prosecutors and financial institutions can work together to prevent, investigate, and prosecute identity theft helps provide answers to the questions and build more effective responses.

The exact impact identity theft has on consumers and businesses each year is difficult to determine.<sup>1</sup> In 2006, the FTC reported that 246,035 consumers filed identity theft complaints with Consumer Sentinel,<sup>2</sup> a decrease of almost four percent from 2005 (FTC, 2007). Of those complainants, fewer people reported in 2006 than in 2005 that they also notified law enforcement about the crime. Nonetheless, criminal justice and financial institution experts note an increase in the number of identity theft incidents brought to their attention over the past five years. Prosecutors who responded to the survey discussed in this report reported a 76.5 percent increase in

<sup>1</sup> Recent data suggest that anywhere from 10 to 15 million people are affected annually, with over \$50 billion in estimated losses to consumers, financial institutions, insurance companies, and others (see FTC, 2003 and Litan, 2007).

<sup>2</sup> Consumer Sentinel is an international, multi-agency project based around an investigative and complaint database that provides information for law enforcement and allows consumers to share information about being victimized by identity theft and other types of fraud. Reporting to Consumer Sentinel is voluntary, therefore there is no way to assess what proportion of identity theft incidents are reported to Consumer Sentinel, or whether that proportion has changed over time.

identity theft victim reports and a 70.6 percent increase in the number of identity theft prosecutions in their jurisdictions over the past five years. Sixty-one percent of financial institution fraud expert respondents reported that identity theft has become more common over the past five years.

Regardless of the exact numbers, identity theft is an increasing concern for consumers as well as law enforcement, financial institutions, and prosecutors. Identity theft perpetrators have evolved from simple schemes involving mail theft or check fraud to complex electronic and digital methods that victimize substantial numbers of people and organizations. One study revealed that, as criminal sophistication has increased, so too has the average loss per identity theft victim (Litan, 2007). Financial institutions and criminal justice professionals have responded to this increased complexity in their work to prevent, deter, investigate, and prosecute identity theft. Law enforcement now pays more attention to identity theft crimes, and officers are more adept at identifying crime suspects, helping victims, and collecting evidence of these crimes. Financial institutions are more aware of the potential for identity theft, and many use security systems and procedures designed to make committing the crime more difficult.

Despite these efforts, identity theft continues to plague financial institutions, the public, and law enforcement. One contributing factor is the definition and understanding of “identity theft,” which varies from state to state. The term can be given different definitions and applications by a financial institution. Legislation that punishes offenders and protects victims differs from state to state, so it is difficult for financial institutions operating in multiple states to uniformly respond to each type of theft. These differing definitions and understanding of what constitutes identity theft color prosecutors’ and financial institutions’ responses in ways that often are incompatible. For example, when a financial institution defines identity theft more narrowly than the criminal statutory definition, financial institutions may treat a fraudulent transaction as a business loss, not recognizing that their customers are crime victims.

Reporting is another factor that complicates identity theft response. Financial institutions prioritize cases differently and use varied practices in response to identity theft. Many financial institutions resist reporting

identity theft incidents to law enforcement or sharing information when law enforcement learns of the crime from other sources. This appears to stem in large part from concern among financial institutions that reporting or providing evidence of identity theft that occurred inside their institution or victimized their customers could negatively impact their reputation—and ultimately their success in the business community. In addition, financial institutions are concerned about violating statutory or regulatory requirements concerning disclosing customer information.

Prosecutors and law enforcement struggle with how to approach victimized financial institutions and their consumers. Prosecutors rely on prompt reporting of crimes and they need to access financial institutions' information, such as account data, video evidence, and witness statements, as evidence of the crimes.

To facilitate dialogue and cooperation between financial institutions and prosecutors, the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice funded a project by the American Prosecutors Research Institute (APRI) in partnership with First Data Corporation and the STAR® Network.<sup>3</sup> The purpose of the project was to pinpoint common problems and obstacles facing financial institutions and prosecutors and share the recommended solutions that they can use to work together successfully.

APRI gathered information on the issues and challenges facing prosecutors and financial institutions from a variety of sources. First, experienced prosecutors and experts from financial institutions participated in a focus group discussion of the key issues and challenges they face. APRI used the information to develop surveys for local prosecutors and financial institutions that provided a national overview of experiences with, and responses to, identity theft crimes.<sup>4</sup> Finally, the survey results were presented to a symposium of experts, who in turn shared their strategies and developed recommendations for their peers. This report represents the culmination of those efforts by presenting recommended strategies for collaboration between prosecutors and financial institutions.

---

<sup>3</sup> First Data Corporation and the STAR® Network provide electronic commerce and payment solutions for businesses and consumers worldwide. The American Prosecutors Research Institute is the research and development division of the National District Attorneys Association.

<sup>4</sup> More information on the project methodology is provided in Appendix A.



# CHALLENGES FACING PROSECUTORS AND FINANCIAL INSTITUTIONS

**M**uch of the challenge related to collaboration between financial institutions and prosecutors is a lack of consistency concentrated in five areas:

- Determining what constitutes identity theft;
- Reporting identity theft crimes;
- Identifying the person or people within an organization who are best situated to respond to inquiries about identity theft incidents;
- Barriers to information sharing; and
- Resources available for investigating and prosecuting identity theft.

The following sections further discuss these issues and include experiences and suggestions from experts to help financial institutions and prosecutors collaborate more effectively. Appendix B contains a list of useful organizations and resources.

## ***Determining What Constitutes Identity Theft***

As anyone who has professional experience handling economic crimes knows, there are many different definitions used to describe identity theft. “Identity theft” is a relatively new term, and laws that specifically criminalize “identity theft” activity are relatively new. Some actions that may previously have been classified as simple theft, forgery, or fraud are now included within the scope of actions that constitute identity theft. There are legal differences across states as to what exactly constitutes identity theft. Financial institution and criminal justice perceptions of what circumstances amount to identity theft—as opposed to other problems such as bad debt, business loss, or other less serious crimes—also differ. Some statutes or financial institutions define “identity theft” as merely the act of acquiring, possessing, using *or* transferring another’s identity or financial information without permission. Other statutes and financial institutions require both the act of acquiring, possessing, using *or* transferring *and* acts of fraud and deceit related to using of another person’s or organization’s identity or financial information. Overall, identity theft may include a few or dozens of actions; affect one or thousands

of consumers; and be local, multi-jurisdictional, or international. It continues to become even more complicated as perpetrators and authorities constantly adapt to each other's strategies.

Defining identity theft was therefore the first issue the team of experts tackled. To consider all points of view, the group decided that using the broadest possible definition would lead to the most comprehensive recommendations. For the purposes of this project, the following definition of identity theft was adopted and used:

*Obtaining, creating, or using another person's (living or dead) or organization's personally identifiable information for any unlawful purpose.*

Any and all references to identity theft in this publication are based on this definition. Although the consensus for this project was to encompass the gamut of possible identity theft types, the simple fact that different definitions exist is important to keep in mind.

### **Reporting Identity Theft**

Prosecutors and financial institutions generally become aware of identity theft incidents through victim complaints or when law enforcement uncovers evidence of the crime while performing other duties. For example, it is common for officers to discover evidence of actual or potential theft during traffic stops, when serving search warrants issued for other crimes, or when performing civil tenant eviction duties. The disparity between the estimated number of victims and the number of documented victims indicates that a relatively small number of identity theft victims report the crime.

Anecdotal experience bears this out. During investigations of other unrelated crimes, law enforcement frequently identifies victims who were previously unaware that their information was compromised. In addition, some identity theft victims might not immediately learn that their identity or financial information was compromised if it is not used to commit fraud until months or years later. These late discoveries complicate efforts to determine the point of compromise and identify which financial insti-

tutions or criminal justice agencies should be involved. Victims also may choose not to report identity theft to law enforcement if they conclude that their financial institution has effectively resolved the problem.

When a victim does decide to contact law enforcement to file a complaint, there is no guarantee that a report will be taken. In 2006, approximately 21 percent of the victims who directly contacted the Federal Trade Commission also notified law enforcement; yet no report was filed (FTC, 2007). Victims need incident reports to access statutory rights granted them by Congress and state laws, such as those granting restitution or financial assistance.<sup>5</sup> As of January 2007, 17 states had laws requiring law enforcement to take identity theft reports from victims. Eight additional states had pending legislation on this subject. Many of those statutes require that law enforcement in the victim's home or employment jurisdiction take a report, even if there is no evidence that the crime occurred in that jurisdiction. The apparent primary purpose of these laws is:

- to assure that victims of identity theft can obtain incident reports from law enforcement without first having to determine which entity has jurisdiction to investigate and prosecute the crimes; and
- to overcome sometimes inconsistent determinations by law enforcement about whether the report should be filed with their department or in another city or state.

These inconsistent determinations are the likely cause of the above-cited statistics about a victim's inability to obtain an incident report.

The majority of statutes that require law enforcement to take identity theft incident reports do not require them to investigate the reported complaints, leaving that decision instead to departments that struggle with limited resources to investigate all reported crimes. Even when required to take incident reports, law enforcement agencies often do not have the resources to conduct thorough investigations, link enough cases together to effectively identify and prosecute groups of active identity thieves, or garner interest at the federal level.

---

<sup>5</sup> For example, 15 USC 1681g(e)(2)(B)(i) allows a business or financial institution, in its discretion, to require the victim to provide a copy of an incident report evidencing the victim's claim to be an identity theft victim (Fair Credit Reporting Act, 2003).

## WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT

Rather than report identity theft to law enforcement, financial institutions often reimburse consumers' losses or conduct internal investigations. There is some indication that such decisions are made because financial institutions conclude that reimbursement is less costly, in terms of out-of-pocket expenses or loss of consumer confidence in their ability to secure personal and financial data.

Once incidents of identity theft do come to the attention of financial institutions or prosecutors, many factors affect their consideration of which cases to pursue, such as resource availability; amount of financial loss to victims, businesses, and financial institutions; victim location; availability of evidence; and whether other financial institutions and/or criminal justice entities are cooperative. APRI asked survey respondents to rate the importance of several factors affecting their decisions about whether or not to pursue a case of identity theft. Although the results represent the views of a small number of financial institutions and prosecutors' offices—and thus cannot be said to accurately represent the entire population—respondents' opinions clearly differ, as indicated in the table below:

% <sup>6</sup>	Financial Institutions (n=87)	Rank	Prosecutors (n=51)	%
70	Potential financial loss to institution	1	Victim cooperation	61
60	Potential reputation loss to institution	2	Number of potential victims	49
56	Potential financial loss to individual victim	3	Potential financial loss to victim	41
48	Potential financial loss to corporate victim	4	Support from law enforcement <sup>7</sup> and financial institutions	39
44	Victim cooperation	5	Potential financial loss to financial institution	29

Given that successful prosecution requires victims to report crimes and continue cooperating whereas competition among financial institutions makes it difficult for them to tolerate financial or reputation losses, it is understandable that prosecutors and financial institutions place different degrees of importance on each factor. Different case prioritization and limited resources complicate the public and private sectors' ability to work

<sup>6</sup> Indicates percent of respondents viewing each factor as "very important."

<sup>7</sup> "Support from law enforcement" and "support from financial institutions" were listed as two separate options on the survey; respondents indicated that they were both equally important.

together efficiently. In addition, the fact that identity theft crimes often span several law enforcement jurisdictions and unrelated financial institutions further complicates efficient cooperation and successful investigation. Thus, intra- and inter-disciplinary cooperation is even more critical.

***Establishing Points of Contact—Identifying the Person or People within an Organization Who Are Best Situated to Respond to Inquiries***

Having the right personal contacts is a simple key element for effective collaboration between organizations. Financial institutions and prosecutors indicate that it is extremely difficult to find the information they need without knowing who to contact. Furthermore, finding that person is often a time-consuming challenge, and contacts will vary as people change positions or assume new responsibilities. In an era of increasingly sophisticated and geographically autonomous criminal activity, successful collaboration depends on developing and maintaining contacts. One person, using a credit card skimmer at a restaurant, can acquire information from credit or debit cards issued to dozens of individuals by dozens of different financial institutions and in turn sell that information to others who then use it in dozens of different cities or states. Seemingly simple actions like this can lead to multi-jurisdictional and inter-institutional cases involving multiple victims, prosecutors' offices, financial institutions, and businesses. Cases borne from electronic strategies such as phishing and pharming,<sup>8</sup> or those carried out by perpetrators located overseas, are even more complicated.

Prosecutors' offices and financial institutions that develop strategies for connecting with each other find that collaboration is a very effective way to conduct identity theft investigations. Networking on an individual basis helps enhance their understanding of each other's goals and needs and helps increase the overall effectiveness of their work. Others establish groups composed of financial institution investigators, law enforcement, and prosecutors that regularly discuss crime trends, specific investigations, and investigative issues as they arise. More than three-quarters of the pros-

---

<sup>8</sup> Phishing and pharming are schemes that deceive consumers into disclosing personal information by, respectively, sending fake e-mails that direct users to enter their information on a fraudulent Web site, or by redirecting Internet traffic from a trusted to a fraudulent site.

ecutors responding to the survey, and most prosecutors on the panel of experts, reported that they established effective personal contacts with financial institutions by reaching out to local financial institution fraud investigators. More than half of the responding prosecutors, and most of the prosecutors on the expert panel, also reported that calling financial institutions' regional or national offices is helpful, and a smaller percentage report that they typically work with a financial institution's legal department. There is not a single strategy guaranteed to get financial institutions and prosecutors to collaborate successfully, but the strategies discussed in later sections provide some suggested approaches to getting started.

### ***Barriers to Information Sharing***

Although prosecutors and financial institutions are very knowledgeable of their own roles, needs, resources, and limitations, discussions at the symposium indicate that they are not aware of how they relate to each other. For instance, financial institutions may not be aware of the evidentiary needs of prosecutors, thus may not assist prosecutors as effectively as they could or may resist prosecutors' requests simply because they do not understand the reasons the requests are made. Whatever the reason, more than half of the prosecutors responding to the survey reported having problems obtaining key information from financial institutions.

Likewise, prosecutors may not be aware of the data privacy restrictions on financial institutions or may inadvertently overburden financial institutions by asking for more information than is necessary. Although prosecutors reported in their survey responses their attempts to make personal contacts with financial institution fraud investigators and legal response teams, financial institution representatives who responded to the survey believe that both law enforcement and prosecutors need additional resources and training on identity theft crimes. This lack of mutual understanding creates one of the largest obstacles for sharing knowledge. Effective cooperation between financial institutions and prosecutors would be greatly enhanced if each had a better understanding of the roles, needs, resources, and limitations faced by their peers in financial institutions, by prosecutors, and by law enforcement.

The multi-jurisdictional nature of banking and identity theft crimes poses additional barriers to information sharing among financial institutions and prosecutors. Most financial institutions operate nationally or regionally, but are domiciled in just one state. Prosecutors' offices prosecute crimes committed within their jurisdictions—strictly defined areas within a city/county, a region within a single state, or, at most, within a state. To effectively prosecute identity theft crimes within their jurisdiction, prosecutors often need records from financial institutions, which may maintain all their records and provide all search warrant/subpoena response services in a single, centralized location. These institutions ask and expect that prosecutors will serve legal process on them at that one address. This enhances efficient records management and response to legal process, but presents some difficulties for prosecutors. Some courts will not issue legal process for an address outside their state's borders. Although prosecutors' offices regularly use search warrants or subpoenas to gather necessary information from financial institutions, these are not always honored when served on the out-of-state organization. Prosecutors also often need information more quickly than many financial institutions can accommodate. Part of this complication stems from prosecutors' uncertainty of what information is available or what they need to prosecute a case, and often they will not know what information is relevant until they actually see it. The search warrant or subpoena, therefore, might ask for all available information.

Financial institutions are rightly concerned with legal issues and how the information they share will be used, but they also express concern about the amount of time it takes them to fulfill information requests (since records are not always kept on-site or may only go back to a certain date). Financial institution representatives at the symposium noted that subpoenas requesting all of the information available for an account might be ignored; instead, they would be more likely to respond to a request that stated exactly what information was needed.

Once requests for records are acknowledged and answered, prosecutors may then need a record custodian from the financial institution to identify the records and testify to the authenticity of the information contained in the records at trial. The need for this financial institution witness is costly

to both the financial institution and taxpayers. The financial institution must pay the employee's salary, and cope with reduced productivity during the one to five (or more) days the employee is out of the office attending a criminal trial. The prosecutor's office (ultimately taxpayers) often fund the travel, lodging and per diem costs. If the prosecutor's office does not have the funds to pay for witness costs, the information they need the witness to authenticate may be inadmissible as evidence. If the financial institution refuses to send a witness to testify at a criminal trial, the financial institution's records will usually be inadmissible, and the prosecutor may be forced to dismiss charges or perhaps the entire case.

Generally, the financial institution's record custodian employee is not needed at the criminal trial to explain the records, but rather only to lay a foundation for the admission of the records into evidence. Although many states require the witness to appear and testify, more than a dozen states allow business records to be admitted without the presence or testimony of a live witness if the records are accompanied by a certification or affidavit establishing their authenticity.

Another challenge for financial institutions, law enforcement, and prosecutors is that they are bound by regulatory and legislative restrictions on what information they are permitted to share with each other. If financial institutions, law enforcement, and prosecutors are able to talk more freely at the outset of investigations about facts, circumstances and trends, it is likely that both financial institutions and prosecutors would be better able to positively resolve their cases.

At face value, it seems beneficial for financial institutions to freely share information not restricted by privacy laws with one another, for instance to identify patterns and new types of fraud and identify and gather evidence on individuals or rings of identity thieves. Federal and state laws concerned with anti-trust and improper reasons for denying customers accounts or credit can put a check on such information sharing among financial institutions. The competitive nature of the banking industry provides more of a disincentive for financial institutions to share information with their competitors. Stress points around information sharing also exist within individual financial institutions. Financial institutions' fraud investi-

gations departments sometimes are at odds with their own marketing departments. For example, some instances of identity theft begin with mail theft, in which the stolen mail includes a financial institution's correspondence with its customers or potential customers. This mail includes customer account statements, pre-approved credit offers, and checks of various types. Financial institution marketing departments are hesitant to abandon this practice because this form of advertisement is a very effective marketing technique. Meanwhile, the fraud investigations departments must investigate fraud arising from theft of such mailings.

Finally, financial institutions are also bound by contractual obligations with various credit card and debit card networks, processors, or large retailers. Those contracts may restrict the information that financial institutions can release to each other or to law enforcement, no matter how beneficial it would be to identity theft investigation and prosecution.

### ***Resources for Investigating and Prosecuting Identity Theft***

Resource scarcity is an ever-present challenge for any organization attempting to become more responsive to identity theft. For prosecutors' offices in particular, budgets are limited, and many offices allocate the bulk of their funding to combating violent and other crimes that pose more immediate dangers to their communities. Although white-collar crimes, such as identity theft, are indeed traumatic and leave lasting effects on victims,<sup>9</sup> few prosecutors' offices have enough funding to focus resources exclusively on specially dedicated identity theft investigators, attorneys, victim advocates, or special prosecution units.

Financial institutions, on the other hand, have more leeway in the use of funds for loss prevention and recovery, but nonetheless may lack a centralized fraud function within the organization. Financial institutions and prosecutors note that they both have been slow to recognize the seriousness of this crime—and slower to act on that recognition once it has occurred. Financial institutions and prosecutors' offices observe that staff

<sup>9</sup> One study revealed that identity theft victims have endured, on average, 265 hours and more than \$3,000 in lost wages, expenses, and medical bills in their efforts to remedy the harm caused. Studies show that in addition to the tangible costs, identity theft victims experience stress, fear, anger, powerlessness, and sleep disturbances. Fifty-four percent of victims reported that they felt unprotected by law enforcement (see Pontell, 2006 and Foley, 2003).

and employees who are responsible for the prevention, investigation, and prosecution of identity theft, as well as victim advocacy, need more training, but resources for training are also scarce. Prosecutors also note that some in law enforcement have responded to limited resources by assessing the skills, specialization, and abilities needed to investigate identity theft or by employing fraud analysts who are specifically trained and assigned to analyze data. Still others have resorted to employing light-duty officers or volunteers to perform tasks that do not require a detective's skills and training, such as collecting records and video from victimized financial institutions or merchants.

### ***Victims' Issues***

Most people instinctively know that avoiding crime victimization altogether is preferable to facing recovery from identity theft victimization—even with excellent victim assistance. Thus, many in financial institutions, law enforcement, and prosecution put at least some effort into educating consumers about identifying and reducing their risks. However, many consumers have not heard the message or need more information about and assistance with protecting themselves. This is especially important when victims are from vulnerable populations—such as children and the elderly—who are less able to recover on their own than other victims, and may even have been victimized by a parent or caregiver.

Victim advocacy is a major challenge facing prosecutors and financial institutions as they address identity theft and related fraud. Although financial institutions often bear the brunt of identity theft-related financial losses, individuals and businesses often spend countless hours trying to rectify the problems created when their identities were stolen. The National Crime Victimization Survey (Bureau of Justice Statistics, 2006) estimates that about one-third of households victimized by identity theft<sup>10</sup> were able to resolve the problem in one day,<sup>11</sup> while more than 30 percent took up to a month and 20 percent needed a month or more.

<sup>10</sup> For the survey, identity theft was defined as either unauthorized use or attempted use of existing credit cards or of existing accounts such as checking accounts, or misuse of personal information to obtain new accounts or loans, or to commit other crimes (Bureau of Justice Statistics, 2006).

<sup>11</sup> The survey did not indicate in what percentage of cases the theft was committed by someone known to the victim. In cases where the perpetrator is known by the victim, it is likely that the amount of time necessary to resolve the theft would be shorter than if the perpetrator was unknown.

This was particularly true in households where someone had experienced theft and misuse of personal information as opposed to credit card theft or use of existing accounts.

For victims to fully recover after suffering from identity theft, they need access to resources and information for preventing, reporting, and responding to identity theft. Both public and private social service organizations such as the FTC, AARP, and Privacyrights.org provide resources for reducing identity theft risk and responding to identity theft after it has occurred. In addition, financial institutions that take action to assist customers frequently focus on measures designed to stop new instances of identity theft. For example, the financial institution may actively monitor customer account, debit, and credit transactions for activity falling outside the norm for that customer. When such activity is spotted, the financial institution will contact the customer to determine whether the activity is fraudulent and if the account should be closed or frozen. Many financial institutions also maintain Web pages that answer common customer questions about preventing and responding to fraud and identity theft. Some financial institutions and prosecutors also participate in public education events, such as shred-a-thons, which invite consumers to bring documents to shred and provide an opportunity to speak with experts about ways to reduce risks of victimization.<sup>12</sup>

After an individual becomes an identity theft victim, both financial institutions and prosecutors' offices focus more on fraud and crime investigation than they do on victim advocacy. Experts note that even when financial institution fraud and law enforcement investigators received training in investigations, few receive any, or very extensive, training focused on providing direct recovery assistance to identity theft victims. Some prosecutors' offices attempt to obtain restitution for victims once their identities are stolen, but it is rare for prosecutors' offices to assign victims' advocates to these types of cases. Experts at the symposium noted that prosecutors frequently have limited resources for victim advocacy, and most use their victim advocates to help victims and families of homicide,

---

12 See, for example, Washington's Law Enforcement Group against Identity Theft (LEGIT), which held a 29-site statewide shred-a-thon where dozens of financial institutions, law enforcement, prosecutors' offices, government, and social service agencies teamed up to educate the public about securing their identities and encouraged people to develop habits for safe handling of identity and financial documents.

## WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT

---

assault, robbery, and other serious crimes cope with victimization and the subsequent investigation and prosecution. Victim advocates are rarely trained to assist victims of financial crimes such as identity theft.

Sending notification to victims that their account has been compromised by fraud or identity theft is another significant issue. A consumer is often not aware of a problem as early as law enforcement or his/her financial institution. When financial institutions learn that a customer's identity or financial information has been accessed without authorization, federal regulations and several state laws require the institution to notify the customer of the breach.<sup>13</sup> Although state laws may be more protective of consumers, there are still gaps that limit how much notification financial institutions and prosecutors can actually carry out. Furthermore, notification is costly. Cases involving dozens if not hundreds or thousands of victims can overwhelm law enforcement and prosecutors with investigative tasks. To then notify the victims involves obtaining names and addresses, sending notification letters, and fielding calls from letter recipients once they are notified—activities and associated costs that impact prosecutors' offices budgets.

---

<sup>13</sup> See 12 C.F.R. Part 30; 12 C.F.R. Parts 208 and 225; 12 C.F.R. part 364; 12 C.F.R. Parts 568 and 570.

# STRATEGIES FOR OVERCOMING BARRIERS TO COOPERATION

As discussed earlier, some of the suggestions offered by identity theft experts may not be relevant or applicable for all financial institutions or prosecutors' offices, but there are significant lessons to be learned. For prosecutors and financial institutions to effectively prevent, investigate, and prosecute identity theft, they must work together to overcome the challenges described in the previous sections. APRI's team of experts identified several key steps that financial institutions and prosecutors' offices can take to achieve that goal:

- Build partnerships, task forces, and collaborative relationships to share knowledge;
- Use existing resources and share new ones through cross-training and linking to existing organizations; and
- Conduct outreach to financial institutions, prosecutors, consumers, businesses, and others who are affected by identity theft.

## ***Build Partnerships, Task Forces, and Collaborative Relationships to Share Knowledge***

Of all of the strategies used by the financial institutions and prosecutors who participated in the symposium, membership with some type of multi-agency/organization task force, working group, or partnership was cited most often and as the most effective strategy for sharing information. Many symposium participants noted that it often was difficult to establish a single point of contact within the financial institution or prosecutor's office, but that once the correct person was identified, they formed relationships that helped them exchange information and resolve investigations more effectively. In particular, prosecutors' offices that maintain a unit dedicated to prosecuting identity theft and other white collar crimes are able to train both public and private sector investigators, develop relationships in the field, educate law enforcement, brainstorm complex cases, review search warrant affidavits, and work with merchants and financial institutions to obtain records relevant to identity theft investigations. For example, in Chicago, Illinois, although identity theft cases

## WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT

---

are initially handled through traditional methods, cases that involve multiple or vulnerable victims, multiple offenders, insiders, or emerging trends are sent to the specialized identity theft unit.

Many prosecutors' offices also practice vertical prosecution for identity theft cases, in which an individual attorney handles a case from start to finish, providing continuity for law enforcement and financial institutions. By adding geographic assignments for attorneys, they have even greater opportunity to create relationships with law enforcement and financial institutions, establishing a team approach to combating the crime.

Although no office or institution had a sure-fire way to develop links and relationships with other organizations, the experts collectively suggested using any and every avenue possible. Those avenues include:

- linking with former law enforcement officials who currently work in the fraud units of financial institutions;
- joining and attending meetings of local financial institution and law enforcement investigators;
- using these groups to share information and intelligence pertinent to investigations and/or current trends in identity theft crime;
- inviting financial institutions and law enforcement to working group meetings;
- encouraging prosecutors to contact local financial institution branches and meet with regional or national private sector fraud experts; and
- having financial institution investigators contact and meet with prosecutors in their jurisdiction.

Other prosecutors and financial institutions ask to appear at advisory group meetings of industry groups, regulatory agencies, and other organizations that deal with consumers who may be affected by identity theft. Working as a group also allows law enforcement, financial institutions, and prosecutors to work collaboratively on identity theft prevention and investigation.

Beyond working in informal groups to share information, regional task forces or working groups can alleviate resource scarcity by consolidating the investigative assets and forensics capabilities of financial institutions

with state, local, and federal law enforcement and prosecutors' offices. The greater the number of organizations and members at the table, the more resources the whole group has access to for addressing the problem. In addition, more members results in less of an overall burden for each individual member or organization.

In New York State, for example, prosecutors from New York City's five boroughs are able to jointly investigate cases that cross jurisdictional lines, therefore address the problem more aggressively. California's Computer and Technology Crime High-tech (CATCH) Response Teams operate collaboratively across several counties to investigate and prosecute fraud and identity theft. Washington State's Law Enforcement Group against Identity Theft (LEGIT), initiated by the state's attorney general, brings together prosecutors, law enforcement, legislators, business and financial industry security professionals, and public and private associations to reduce identity theft in the state. Including legislators in discussions with those on the front lines of combating identity theft creates the opportunity to introduce measures that ease the process.

Symposium attendees cited a number of task forces, partnerships, or allied organizations. Prosecutors reported participating in task forces comprised of local business organizations, communications, and utility companies; other public entities such as coroners' offices and departments of motor vehicles; and county agencies on aging, consumer protection, and licensing and inspections. They also reported collaborating formally and informally with various state and federal agencies including the Federal Bureau of Investigation, Internal Revenue Service, Federal Trade Commission, U.S. Postal Inspection Service, U.S. Immigration and Customs Enforcement, U.S. Marshals, Social Security Administration, state attorneys general, as well as with surrounding jurisdictions, and state and local law enforcement.

Some jurisdictions have arrangements with the local U.S. Attorney's Office, taking a tag-team approach to prosecution where offenders are encouraged to plead in state court to avoid federal prosecution, thus reducing the time commitment necessary to process the case while ensuring the offender will be punished. In addition, the U.S. Secret

Service was mandated by the *Patriot Act* (USA PATRIOT Act, P.L. 107-56, 2001) to establish a nationwide network of Electronic Crimes Task Forces that team all levels of law enforcement with prosecutors, academia, and the private sector. There are currently 24 regional locations, and the Secret Service expects this network to continue to grow.

Financial institutions are also active in a multitude of associations, networks, and working groups. Some of the most notable and well-known include the Association of Certified Fraud Examiners, Banking Industry Technology Secretariat (now known as BITS)/Financial Services Roundtable, and the International Association of Financial Crimes Investigators. These entities provide leadership, establish priorities, and develop recommendations for the financial services industry as well as liaison with law enforcement and government organizations. Some financial institutions also participate in organizations such as Fraud-Net to share information and alerts about identity theft and fraud across organizations, states, and the country. Some of these organizations are organized primarily by financial institution executives. Others are equally inclusive of public and private entities and may include investigators, fraud examiners, attorneys, other bank employees, and university professors or other researchers as members.

Although many of the above-mentioned organizations have mandates to address consumer protection from fraud, electronic or white-collar crimes other than identity theft, they are all interested in working collaboratively to fulfill their missions and can provide invaluable information and resources to even the most experienced professionals. For an extended list of existing task forces, associations, and networks; local, state, federal, and private industry resources; contact information; and Web links, please refer to Appendix B.

### ***Develop Mutual Understanding of Information Needs and Restrictions through Cross-Training***

As detailed above, lack of knowledge on the part of financial institutions and prosecutors about the problems each faces is a difficult barrier. Cross-training prosecutors and financial institutions as well as law

enforcement and merchants gives all entities involved in identity theft prevention, investigation, and prosecution a holistic and well-rounded view of their role in the process and the needs of their partners. For example, a clear understanding of how the state or financial institution defines and addresses identity theft makes it easier for the financial institution and prosecutor to know which cases are mutually significant and what information and action each needs from the other to resolve investigations successfully. Once the two align their priorities, financial institutions can confidently conduct much of the legwork for investigations, knowing that the cases are solid and more likely to be filed when prosecutors do not have to backtrack and gather additional evidence.

Conversely, prosecutors can validate the financial institution's hard work by keeping them informed of progress and case outcomes. In Suffolk County, Massachusetts, banks, insurance companies, fraud investigators, and prosecutors in the Boston area are cross-trained, allowing each party to share their needs and assets with each other and helping to streamline identity theft prevention, investigation, and prosecution.

Larger financial institutions and prosecutors' offices often help smaller offices and organizations by sharing knowledge and reaching out to provide support when necessary. Since identity theft is a "boundary-less" crime, smaller communities may be affected just as much if not more due to the limitations on their resources. The multi-jurisdictional nature of identity theft also strongly lends itself to alignment with regional and national entities. The agencies and task forces mentioned in the previous section have considerable knowledge and resources and often are willing to provide information, support, networking, and training to other parts of the criminal justice system. In addition, associations can be helpful in developing and organizing trainings. For example, the California District Attorneys Association provides an annual identity theft training, which supplies prosecutors with resources for investigation and trial preparation.

### ***Educate Constituent Groups***

A thief cannot steal an identity if he or she cannot first find personal and financial information belonging to a potential victim. Individuals who develop habits to secure their identities and protect themselves as much

as possible from theft and abuse are better able to avoid becoming identity theft victims. Since neither financial institutions nor prosecutors can identify and bring to justice all identity thieves, it is generally agreed that prevention is the first step in addressing identity theft.

Prosecutors and financial institutions should continually encourage the public to take steps to reduce their risk of becoming identity theft victims. Similarly, prosecutors and financial institutions should encourage victims to report identity theft crimes, since the rights provided under the Fair Credit Reporting Act and many state statutes are not triggered until victims have obtained incident reports documenting their victimization by an identity thief. Financial institutions can increase consumer confidence in their organizations through outreach and education on identity protection. Similarly, prosecutors fulfill their duties to their communities by conducting or participating in public education focused on preventing and prosecuting identity theft. Educating the consumer and business communities about identity theft and what they can do to prevent it is a proactive approach that builds on and strengthens allied partnerships. This has been particularly important when large entities such as universities are victimized and hesitant to request outside help because they do not want to alarm the public. Reliable and trustworthy support from financial institutions and prosecutors encourages these organizations to be active partners in preventing and responding to identity theft, protecting many more consumers from becoming victimized.

## CONCLUSION

One of the most important lessons learned from the symposium and other contacts with experienced identity theft professionals is that the problem is constantly changing. The information provided in this document is intended to educate prosecutors and financial institution professionals about each other's needs and experiences so that they can work together more effectively; however, it is important to note that those needs and experiences will change. To continue effectively preventing, investigating, and prosecuting identity theft, prosecutors and financial institutions must continue to work together, sharing information about the methods perpetrators use, ways to help victims, and promising practices that make their work easier and more effective. APRI encourages financial institution professionals and prosecutors to continue sharing information with each other, as well as with national organizations like APRI and the Bureau of Justice Assistance so that information can be disseminated. Sharing news of emerging methods of identity theft; uses of information; prevention, detection, investigation, and prosecution strategies; new task forces, associations, and working groups; and any other relevant information will strengthen the overall ability of prosecutors and financial institutions to successfully combat identity theft.



## REFERENCES

Bank holding companies and change in bank control (Regulation Y) (1997). 12 C.F.R. Part 225. (LexisNexis).

Disclosures to consumers (2003). 15 U.S.C. Part 1681. (LexisNexis).

Federal Trade Commission (2003). Federal Trade Commission – Identity theft survey report. Synovate: Online. Available: [http://www.consumer.gov/idtheft/pdf/synovate\\_report.pdf](http://www.consumer.gov/idtheft/pdf/synovate_report.pdf) [3 Apr. 2007].

Federal Trade Commission (2007). Consumer fraud and identity theft complaint data January – December 2006. Consumer Sentinel: Online. Available: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf> [26 Mar. 2007].

Foley, J., & Foley, L. (2003). Identity theft: The aftermath 2003. San Diego, CA: Identity Theft Resource Center: Online. Available: [http://www.idtheftcenter.org/artman2/uploads/1/The\\_Aftermath\\_2003.pdf](http://www.idtheftcenter.org/artman2/uploads/1/The_Aftermath_2003.pdf) [25 Mar. 2007].

Litan, A. (2007). The truth behind identity theft numbers. Gartner Research Group: Stamford, CT.

Membership of state banking institutions in the federal reserve system (Regulation H) (1998). 12 C.F.R. § 208. (LexisNexis).

Pontell, H. N. (2006). Stolen identities: A victim survey. Panel discussion presented at Annual Conference of the National Institute of Justice, Washington, DC.

Safety and soundness guidelines and compliance procedures (1995). 12 C.F.R. Part 570. (LexisNexis).

Safety and soundness standards (1995). 12 C.F.R. Part 30. (LexisNexis).

## **WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT**

---

Security Procedures (1991). 12 C.F.R. Part 568. (LexisNexis).

Standards for safety and soundness (1998). 12 C.F.R. Part 364. (LexisNexis).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (2001). P.L. 107-56. 115 Stat 272. (LexisNexis).

## APPENDIX A: METHODOLOGY

The focus group, which included representatives from local prosecutors' offices, financial institutions, and law enforcement, among others, worked together to examine key issues in combating identity theft. The discussion focused first on understanding identity theft—that is, identifying common types of identity theft, victims, and perpetrators and the barriers and problems with identifying, preventing, and responding to identity theft and related fraud. Further dialogue concentrated on the resources available to prosecutors and financial institutions for addressing identity theft and opportunities for collaboration and information sharing between groups. The information collected from these discussions helped frame the questions used in the survey of prosecutors and financial institutions.

Surveys were distributed to 307 prosecuting attorneys' offices and more than 8,000 financial institution personnel. Respondents were asked to provide answers to a range of questions addressing the scope of the identity theft problems they encounter, practices used in responding to identity theft, barriers to recognizing and preventing identity theft, resources, and strategies for information sharing and coordination. Responses were collected from 87 financial institution representatives and 51 prosecutors' offices. Although the low response rates (one percent for financial institutions; 17 percent for prosecutors) does not allow for meaningful analysis of the state of identity theft nationwide, it provided valuable information for understanding the scope of the problem and guiding expert discussions at the symposium.

Participants at the symposium were presented with results of the survey to further discuss the scope of the problem as well as current practices, barriers, challenges, and strategies for overcoming those barriers. They were asked to share promising approaches used by their financial institutions or local jurisdictions in order to generate recommendations for more effective responses to identity theft.



# APPENDIX B: CONTACTS AND RESOURCES

## **Federal Agencies**

### **Department of Homeland Security**

<http://www.dhs.gov/index.shtm>

### **U.S. Secret Service**

<http://www.secretservice.gov/>

Established solely to suppress the counterfeiting of U.S. currency and has now extended its services to investigate cases that involve some form of electronic crime.

### **Department of Justice**

<http://www.usdoj.gov/ittf>

### **Bureau of Justice Statistics**

<http://www.ojp.usdoj.gov/bjs>

Collects, analyzes, publishes, and disseminates information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. It has revised its National Crime Victimization Survey (NCVS) to include data on identity theft victimization and its consequences.

### **Federal Bureau of Investigations**

<http://www.fbi.gov>

Includes financial crimes investigations that are primarily focused on corporate fraud, health care fraud, mortgage fraud, identity theft, insurance fraud, mass marketing fraud, and money laundering.

### **National Institute of Justice**

<http://www.ojp.usdoj.gov/nij>

The research, development, and evaluation agency of the U.S. Department of Justice dedicated to researching crime control and justice issues. As part of its strategic planning, NIJ has identified high-priority research, development, and evaluation needs of the field to

include an expansion of knowledge on nature of white collar crime, identity theft, and elder fraud and strategies to prevent victimization.

### **Office of Legal Policy**

<http://www.usdoj.gov/olp>

Responsible for developing, coordinating, and implementing policies of major initiatives. The assistant attorney general and OLP have played a key role in the assessment of federal identity theft-related efforts and the development of policies designed to improve those efforts.

### **Office of Victims of Crime**

<http://www.ojp.usdoj.gov/ovc>

Provides substantial funding to state victim assistance and compensation programs that help victims heal and supports trainings designed to educate criminal justice and allied professionals regarding the rights and needs of crime victims. OVC will continue to take a prominent role in federal efforts addressing identity theft victimization and to assist law enforcement, prosecutors, victim advocates, and state agencies through education, outreach, research, and innovative programs to help victims recover.

### **National Criminal Justice Reference Service**

<http://www.ncjrs.gov>

Provides services and resources of criminal justice related information to anyone interested in crime, victim assistance, and public safety including policymakers, practitioners, researchers, educators, community leaders, and the general public. The topical resource on identity theft contains the following information: facts and figures, legislation, publications, programs, training and technical assistance, grants and funding, and related resources.

### **United States Attorneys**

<http://www.usdoj.gov/usao>

Serve as the chief federal law enforcement officers of the United States within their particular jurisdictions. Although the distribution of case-load varies between districts, each has every category of cases, including fraud-related crimes.

**United States Trustee Program**

<http://www.usdoj.gov/ust>

Responsible for overseeing the administration of bankruptcy cases and private trustees. The U.S. attorney general appoints a separate U.S. trustee for each of the 21 geographical regions. Each trustee is responsible for maintaining and supervising a panel of private trustees for Chapter 7 bankruptcy cases. Detecting and combating bankruptcy fraud is a U.S. Trustee Program priority.

**Department of State**

[http://www.travel.state.gov/passport/passport\\_1738.html](http://www.travel.state.gov/passport/passport_1738.html)

Provides information and services to American citizens about how to obtain, replace or change a passport and the protection of fraud and identity theft when a passport is replaced or changed.

**Department of the Treasury**

<http://www.ustreas.gov>

**Office of Critical Infrastructure Protection and Compliance Policy**

<http://www.treas.gov/offices/domestic-finance/financial-institution/cip/>

A task force office organized on the federal level to coordinate the fight against identity theft.

**Internal Revenue Service**

<http://www.irs.gov>

Serves the public with tax collection and tax law enforcement, including protecting the public from scams and cons.

**Federal Deposit Insurance Corporation**

<http://www.fdic.gov>

Preserves and promotes public confidence in the U.S. financial system by insuring deposits in financial institutions and identifying, monitoring, and addressing risks to the deposit insurance funds.

### **Federal Trade Commission**

<http://www.ftc.gov/idtheft>

Ensures compliance with consumer protection and business competition laws and maintains several Web sites focused on “hot topics” of interest to the public. The Identity Theft Web site provides information to help consumers deter, detect, and defend against identity theft including links to government reports and congressional testimony, law enforcement updates, and other identity theft sites.

### **Securities and Exchange Commission**

<http://www.sec.gov/about/whatwedo.shtml>

Protects investors, maintains fair, orderly, and efficient markets, and facilitates capital formation.

### **Social Security Administration/Office of Inspector General**

<http://www.ssa.gov/oig>

Provides identity theft hotline numbers, information on reclaiming identity, Social Security card replacement, information on correcting records, and how to obtain a new Social Security number.

### **U.S. Postal Inspection Service**

<http://www.usps.com/postalinspectors>

Responsible for protecting the nation’s mail system from criminal misuse; leaders in the fight against identity theft.

### **Federal Laws**

The following are federal credit, false identification, identity theft, and privacy laws pertaining to the prevention, investigation, and prosecution of identity theft. This information is freely available to the public. Among the Web sites where this information and other resources may be found are the FTC: [www.ftc.gov](http://www.ftc.gov); EDUCAUSE: [www.educause.edu](http://www.educause.edu); and at [www.llrx.com/features/idtheftguide.htm](http://www.llrx.com/features/idtheftguide.htm).<sup>14</sup>

### **Federal Credit Laws**

Consumer Credit Protection Act

<sup>14</sup> This information and the links were current as of 2/12/07. APRI is not responsible for the content of the sites unless otherwise noted.

Fair Credit Reporting Act:  
Fair and Accurate Credit Transactions Act (FACTA) of 2003  
Fair Credit Billing Act  
Truth in Lending Act  
Electronic Funds Transfer Act

**Federal False Identification Laws**

False Identification Crime Control Act of 1982  
Internet False Identification Act of 2000

**Federal Identity Theft Laws**

Identity Theft and Assumption Deterrence Act  
Identity Theft Penalty Enhancement Act  
Fair and Accurate Credit Transactions Act of 2003  
Fair Debt Collections Practices Act  
Identity Theft Consumer Notification Act  
Identity Theft Prevention Act of 2005

**Federal Privacy Laws**

Privacy Act of 1971  
Drivers Privacy Protection Act of 1994  
Health Insurance Portability and Accountability Act of 1996 (HIPAA)  
Gramm-Leach-Bliley Act of 1999 (also known as the Financial Services  
Modernization Act of 1999)  
Social Security Number Confidentiality Act of 2000

**Task Forces**

The list of task forces below is organized by region. They involve a variety of public and private entities and focus on a range of issues from consumer protection to multi-agency prosecution of identity theft and other high-tech, organized, and fraud-related crimes.

Search for the task forces in your region to find one to join, or contact any organization whose model may be used to create one in your area. Entries annotated with [ECTF] are part of the network of task forces established by the U.S. Secret Service to help prevent and prosecute

identity theft and related crimes. More information is available at:  
<http://www.secretservice.gov/ectf.shtml>.

### **WEST**

#### **Bay Area Electronic Crimes Task Force [ECTF]**

A group of federal, state, and local investigators and corporate partners lead by the U.S. Secret Service focused on attacking high technology crime affecting Bay Area companies.

Phone: (415) 744-9026

Fax: (415) 744-9051

E-mail: [sfoectf@einformation.usss.gov](mailto:sfoectf@einformation.usss.gov)

#### **California District Attorneys Association High Tech Committee**

Serves as a source of continuing legal education and legislative advocacy for its membership and provides a forum for the exchange of information and innovation in the criminal justice field.

731 K Street, 3rd Floor

Sacramento, CA 95814

Phone: (916) 443-2017

Fax: (916) 443-0540

<http://www.cdaa.org>

#### **Computer and Technology High-Tech Response Team (CATCH)**

A multi-agency task force formed in June 2000 to apprehend and prosecute all criminals who use technology to prey on the citizens of San Diego, Imperial, and Riverside Counties.

Keith Burt, Project Director, or

Commander James Ray, Law Enforcement Coordinator

330 W. Broadway, Ste. 750

San Diego, CA 92101

Phone: (619) 531-3660

E-mail: [kburt@catchteam.org](mailto:kburt@catchteam.org)

E-mail: [jray@catchteam.org](mailto:jray@catchteam.org)

Phone: (619) 531-3660  
<http://www.catchteam.org>

**Hawaii Identity Theft & Financial Crimes Task Force**

Provides information for consumers to reduce their chances of becoming a victim and minimizing the damage.

Phone: (800) 464-4644 (toll free)  
[http://www.hawaii.gov/dcca/quicklinks/id\\_theft\\_info/](http://www.hawaii.gov/dcca/quicklinks/id_theft_info/)

**Las Vegas Electronic Crimes Task Force [ECTF]**

Hosted by the U.S. Secret Service and the Las Vegas Metropolitan Police Department Cybercrimes Unit, the LVECTF combats computer-related crimes and offers the community a resource for local contacts, cyber security concerns, and information on preventing theft.

Phone: (702) 388-6571  
Fax: (702) 388-6668  
E-mail: [lasectf@einformation.uss.gov](mailto:lasectf@einformation.uss.gov)

**Los Angeles Electronic Crimes Task Force [ECTF]**

Since its creation on October 24, 2002, the Los Angeles Electronic Crimes Task Force (LAECTF), which includes six federal, state, and local law enforcement agencies, has provided training and technical expertise in e-commerce, network security, and digital data recovery to the industry, academia, and law enforcement communities.

Phone: (213) 894-4830 (General Office for USSS)  
Phone: (213) 533-4650 (Direct Phone for ECTF)  
E-mail: [laxectf@einformation.uss.gov](mailto:laxectf@einformation.uss.gov)

**Northwest Fraud Investigators Association**

Serves to secure the full cooperation of all those interested in the location, prosecution, and conviction of all persons defrauding the public.

Doug Jordan, President  
Eugene Police Department

Bethel Public Safety Station  
646 Hwy 99 N.  
Eugene, OR 97401  
Phone: (541) 682-6235  
E-mail: [Doug.r.jordan@ci.eugene.or.us](mailto:Doug.r.jordan@ci.eugene.or.us)  
<http://www.nwfia.org/index.html>

**Rapid Enforcement Allied Computer Team Task Force**

A partnership of 16 local, state, and federal agencies, with the Federal Bureau of Investigations designated as the lead agency.

1919 South Bascom Ave, 4th Floor  
Campbell, CA 95008  
Phone: (408) 558-1198  
Fax: (408) 558-3977  
E-mail: [reactsj@reacttf.org](mailto:reactsj@reacttf.org)

FBI San Jose Office  
Phone: (408) 998-5633  
<http://www.reacttf.org>

**Sacramento Valley Hi-Tech Crimes Task Force**

Focuses on multi-jurisdictional investigations; tracking and disruption of commerce involving stolen goods; and investigation and prosecution of those engaged and participating in white-collar crime, organized crime, crimes against persons, and fraud when high technology or identity theft is a factor.

4510 Orange Grove Ave  
Sacramento, CA 95841  
Phone: (916) 874-3000  
E-mail: [info@cachitechcops.org](mailto:info@cachitechcops.org)  
<http://www.sachitechcops.org/>

**Seattle Electronic Crimes Task Force [ECTF]**

Phone: (206) 220-6800  
E-mail: [seaecwg@einformation.usss.gov](mailto:seaecwg@einformation.usss.gov)

**Southern California High Tech Task Force (SCHTTF)**

A collaborative effort of local, county, state and federal law enforcement agencies working to combat high tech crime involving the Internet, intellectual property, computer equipment, emerging technologies, theft of identity information and numerous other high tech crimes.

High Technology Crime Division  
Los Angeles County District Attorney's Office  
201 N. Figueroa Street, Suite 1200  
Los Angeles, CA 90012  
Phone: (213) 580-3272  
Fax: (213) 250-8769  
E-mail: [jmcgrath@lacountyda.org](mailto:jmcgrath@lacountyda.org)  
<http://da.co.la.ca.us/htcu.htm>

**Washington County Sheriff's Office**

Fraud and Identity Theft Enforcement Team  
Rob Gordon, Sheriff  
215 SW Adams, MS 32  
Hillsboro, OR 97123  
Fax: (503) 846-2733  
<http://www.co.washington.or.us/sheriff/investig/fraud.htm#other>

**SOUTH**

**Atlanta Electronic Crimes Task Force [ECTF]**

The goal of the Atlanta Electronic Crimes Task Force is to facilitate the flow of information between the Secret Service's partners by sharing information and developing methods and means to better investigate, identify, and combat electronic crimes.

Phone: (404) 331-6111  
E-mail: [atlectf@einformation.uss.gov](mailto:atlectf@einformation.uss.gov)

**Birmingham Electronic Crimes Task Force [ECTF]**

The Birmingham Electronic Crimes Task Force seeks to prioritize investigative cases that involve some form of electronic crime.

Phone: (205) 731-1144

E-mail: [bhmcw@einformation.usss.gov](mailto:bhmcw@einformation.usss.gov)

**Charlotte Metro Electronic Crimes Task Force [ECTF]**

A multi-agency task force created to investigate and combat electronic and financial crimes. The task force concentrates its efforts on the investigation of cyber crime, computer crimes, network intrusions, online enticements, hacking cases, Web site defacements, and identity theft relative to the security of financial and personal information.

Phone: (704) 442-8370

Fax: (704) 442-8369

E-mail: [cltctf@einformation.usss.gov](mailto:cltctf@einformation.usss.gov)

**Georgia State Attorney's Office STOP IT**

A public/private partnership set up by the Attorney General of Georgia to provide information for Georgia consumers with preventive measures and tips on how to react to identity theft.

Javoyne Hicks

Office of the Attorney General

Consumer Interests Section

40 Capitol Square S.W.

Atlanta, GA 30334

Phone: (404) 651-9340

[http://www.state.ga.us/ago/consumer\\_resources.html](http://www.state.ga.us/ago/consumer_resources.html)

**Houston Electronic Crimes Task Force [ECTF]**

Phone: (713) 868-2299

Fax: (713) 868-5093

E-mail: [hoeuctf@einformation.usss.gov](mailto:hoeuctf@einformation.usss.gov)

**Miami Electronic Crimes Task Force [ECTF]**

Investigates cyber crime, computer crimes, network intrusions, online enticements, hacking cases, Web site defacements, and identity theft of financial and personal information.

Phone: (305) 863-5400

E-mail: [miaectf@einformation.usss.gov](mailto:miaectf@einformation.usss.gov)

**North Texas Electronic Crimes Task Force [ECTF]**

A partnership formed between law enforcement, private corporations, and academia.

Irvine, TX 75062-2752

Phone: (972) 868-3200

E-mail: [dalectf@einformation.usss.gov](mailto:dalectf@einformation.usss.gov)

**Orlando Electronic Crimes Task Force [ECTF]**

An alliance of federal, state, county and local law enforcement; private industry; and academia working to prevent attacks on the nation's critical infrastructure, particularly in the electronic or cyber arena, through information sharing, criminal investigations, computer forensics and training.

Phone: (407) 648-6333

E-mail: [orlecwgf@einformation.usss.gov](mailto:orlecwgf@einformation.usss.gov)

**South Carolina Electronic Crimes Task Force [ECTF]**

The South Carolina Electronic Crimes Task Force (SC-ECTF) and the South Carolina Law Enforcement Division Computer Crime Center, key partners since 2003, are the state's focal points for a number of local, state, and federal computer crime law enforcement efforts.

Phone: (803) 772-4015

E-mail: [cscectf@einformation.usss.gov](mailto:cscectf@einformation.usss.gov)

**MIDWEST**

**Chicago Electronic Crimes Task Force [ECTF]**

A strategic alliance of federal, state, and local law enforcement agencies, private industry, academia, and private sector technical experts working together to confront and suppress technology-based criminal activity that endangers the integrity of the nation's financial payments systems and poses threats against the nation's critical infrastructure.

## **WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT**

---

Phone: (312) 353-5431

Fax: (312) 353-1225

### **Cleveland Electronic Crimes Task Force [ECTF]**

Provides a forum for information exchange on a broad range of information technology topics. Members come from diverse manufacturing and critical infrastructure industries, government agencies, academic institutions, and enforcement bureaus within Northern Ohio.

Phone: (216) 706-4365

Fax: (216) 706-4445

E-mail: cleectf@einformation.uss.gov

### **Kentucky Electronic Crimes Task Force [ECTF]**

Focuses its efforts on the investigation of cyber crime, computer crimes, network intrusions, hacking cases, and identity theft relative to the security of financial and personal information. Task force members include federal and local law enforcement, financial institutions, academia, as well as members from the private sector involved in computer security.

Phone: (502) 582-5171

E-mail: louecwg@einformation.uss.gov

### **Minnesota Electronic Crimes Task Force [ECTF]**

Serves Minnesota, North Dakota, and South Dakota.

Phone: (612) 348-1800

E-mail: mspecwg@einformation.uss.gov

### **Minnesota Financial Crimes Task Force**

Authorized and funded by the Minnesota Legislature to investigate identity theft and financial crimes throughout the state.

Chris Abbas, Commander

P.O. Box 21007

Columbia Heights, MN 55421

Phone: (763) 502-7756

Fax: (763) 502-7758

**Ohio Organized Crime Investigations Commission**

Organizes personnel who are involved with combating organized retail crime throughout North America.

Organized Retail Crime Committee

Kenneth B. Marshall, Executive Director

Attorney General's Office of Ohio

Phone: (614) 227-1000

E-mail: [kmarshall@napri.org](mailto:kmarshall@napri.org)

<http://www.ag.state.oh.us/le/investigation/oocic.asp>

**Oklahoma Electronic Crimes Task Force [ECTF]**

Concentrates on the investigation of cyber crimes, computer crimes, network intrusions, online enticements, hacking cases, and Web site defacements relative to the security of financial and personal information.

Members include federal, state, and local law enforcement; financial institutions; academia; and members of the private sector involved in computer security.

Phone: (405) 810-3000

E-mail: [okcecwge@einformation.uss.gov](mailto:okcecwge@einformation.uss.gov)

**NORTHEAST**

**Bucks County Older Adult Abuse Task Force**

Launched a Fraud Alert program that delivers monthly e-mail alerts to older adults, caregivers, and community groups. Web site provides information on why older adults are vulnerable to financial abuse and how to recognize financial elder abuse.

<http://crimesagainstolderadultsbucks.org/>

Network of Victim Assistance (NOVA)

Coordinator of Elder Abuse Services

Phone: (800) 675-6900 or (215) 343-6543

## **WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT**

---

Bucks County Area Agency on Aging (AAA)

Phone: (215) 348-0510

Bucks County Consumer Protection

Phone: (215) 348-6060

Bucks County District Attorney's Office

Phone: (215) 348-6344

### **Maryland Electronic Crimes Task Force [ECTF]**

A partnership between the Secret Service, other law enforcement agencies, academia, and the private sector. The success of the task force is based on trusted partnerships with the focus on prevention and criminal investigations.

Phone: (443) 263-1000

Fax: (443) 263-1100

E-mail: [balecwg@einformation.usss.gov](mailto:balecwg@einformation.usss.gov)

### **New England Electronic Crimes Task Force [ECTF]**

Facilitates skills sharing between member partners and provides tools, services, deliverables, and processes that are designed to meet the needs of the community.

Phone: (617) 565-5640

Fax: (617) 565-5659

E-mail: [bosectf@einformation.usss.gov](mailto:bosectf@einformation.usss.gov)

### **New York/New Jersey Electronic Crimes Task Force [ECTF]**

An alliance of the U.S. Secret Service; private industry; academia; and other local, state, federal, and international law enforcement officials working to protect the nation's critical infrastructure. Uses the latest in high-tech equipment to deter, detect, and respond to criminal threats.

Phone: (718) 840-1220

Fax: (718) 840-1229

E-mail: [nyectf@usss.dhs.gov](mailto:nyectf@usss.dhs.gov)

**Philadelphia Area Electronic Crimes Task Force [ECTF]**

Began in 2003 as the Philadelphia Electronic Crimes Working Group. Since its establishment, the PAECTF continues to build partnerships within the Philadelphia district with members from law enforcement, private industry, and academic institutions.

Phone: (215) 861-3300

E-mail: [phlectf@einformation.uss.gov](mailto:phlectf@einformation.uss.gov)

**Pittsburgh Electronic Crimes Task Force [ECTF]**

A network of law enforcement, academia, and business professionals sharing information and resources to create a more secure electronic environment and apprehend those who violate that security. Provides technical support for local investigators and training for law enforcement and businesses to better understand the restrictions and requirements involved in cyber investigation.

Phone: (412) 281-7825

E-mail: [tri-cin@uss.dhs.gov](mailto:tri-cin@uss.dhs.gov)

**State of Maryland Identity Task Force**

Office of the Attorney General

200 St. Paul Place

Baltimore, MD 21202

Phone: (410) 528-8662 or (888) 743-0023 (toll free)

<http://www.oag.state.md.us/Consumer/index.htm>

**Upstate New York Electronic Crimes Task Force [ECTF]**

A partnership of federal, state, and local law enforcement agencies, prosecutors, private sector companies, and academia incorporating cyber crime security assets from four geographical regions of Upstate New York (Buffalo, Rochester, Syracuse and Albany) into a centralized investigative unit administered by the Secret Service.

Phone: (716) 551-4401

E-mail: [bufactf@einformation.uss.gov](mailto:bufactf@einformation.uss.gov)

**Virginia Metro Richmond ID Theft Task Force**

2720 Enterprise Parkway, 2nd Floor  
Richmond, VA 23284  
Fax: (804) 418-6198  
<http://www.fraudandidentitythefttaskforce.com>

**Washington-Metro Electronic Crimes Task Force [ECTF]**

Phone: (202) 406-8000  
Fax: (202) 406-8803  
E-mail: [wfoectf@einformation.uss.gov](mailto:wfoectf@einformation.uss.gov)

**State Government Resources**

**National Conference of State Legislatures**

<http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm>

Identity theft statutes by state. Lists statutory citations and associated penalties. The site also includes state legislation enacted in 2004 on identity theft, with descriptions and links to bills.

**Florida Attorney General**

<http://myfloridalegal.com/identitytheft>

The state of Florida's Identity Theft Response Center. Resources include a theft victim kit, statistics, and information on preventing theft.

**State Laws on Criminal Identity Theft, Credit Information Blocking, Fraud Alerts, and Social Security Numbers**

[www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/laws.html](http://www.ftc.gov/bcp/edu/microsites/idtheft/law-enforcement/laws.html)

**Associations and Non-Governmental Organizations**

The organizations listed here include associations, partnerships, and other non-governmental organizations that provide networking, resources, and representation for public agencies, private organizations and consumers.

**American Bankers Association**

Represents banks of all sizes on issues of national importance for financial institutions and their customers. Its membership, which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks, makes ABA the largest banking trade association in the country.

1120 Connecticut Avenue, N.W.  
Washington, DC 20036  
Phone: (800) BANKERS  
<http://www.aba.com>

**AARP (Formerly the American Association for Retired People)**

The leading nonprofit, nonpartisan membership organization for people age 50 and over in the United States.

Phone: (888) 687-2277  
601 E Street NW  
Washington, DC 20049  
<http://www.aarp.org>

**Association of Certified Fraud Examiners**

The mission of the Association of Certified Fraud Examiners is to reduce the incidence of fraud and white-collar crime and to assist its members in its detection and deterrence.

World Headquarters - The Gregor Building  
716 West Ave  
Austin, TX 78701-2727 USA  
Phone: (800) 245-3321 (USA & Canada only) or  
(512) 478-9000  
Fax: (512) 478-9297  
<http://www.acfe.com/home.asp>

**Bank Administration Institute (BAI)**

BAI reaches thousands of financial services professionals each year to

deliver content designed around critical business needs and to facilitate vital connections between financial services professionals, industry experts and solutions providers.

One N. Franklin  
Suite 1000  
Chicago, IL 60606-3421  
Phone: (312) 683-2464  
Fax: (312) 683-2373  
<http://www.bai.org/about>

### **Better Business Bureau**

Provides identity theft-related resources, research, and news for consumers and businesses.

<http://www.bbb.org/>

### **Banking Industry Technology Secretariat (BITS)/Financial Services Roundtable**

BITS is a nonprofit, CEO-driven industry consortium whose members are 100 of the largest financial institutions in the United States. BITS was formed by the CEOs of these institutions to serve as the strategic “brain trust” for the financial services industry in the e-commerce, risk management, payments and technology arenas. BITS addresses emerging issues where financial services, technology and commerce intersect acting quickly to address problems and galvanize the industry.

Main Office  
1001 Pennsylvania Avenue NW  
Suite 500 South  
Washington, DC 20004  
Tel: (202) 289-4322  
Fax: (202) 628-2492  
[bits@fsround.org](mailto:bits@fsround.org)  
<http://www.bitsinfo.org/>

### **FIST-Oregon Bankers**

Oregon's only full-service trade association representing state and national commercial banks, thrifts, and saving banks chartered to do business in Oregon.

Doug Kidder  
VP & Mgr of Corporate Security & Loss Prevention  
Umpqua Bank  
Tigard, OR 97470  
Phone: (503) 727-4286  
Fax: (503) 727-4273  
E-mail: dougkidder@umpquabank.com  
<http://www.oregonbankers.com>

### **Identity Theft Resource Center (ITRC)**

ITRC is a national organization dedicated to helping people prevent and recover from identity theft. Resources include FAQs, scams and consumer alerts, current laws, and guides for organizing an identity theft case.

<http://www.idtheftcenter.org/>

### **Identity Theft Assistance Center (ITAC)**

A cooperative initiative founded by the financial services industry to provide a free victim assistance service for customers of member companies. This organization is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation sponsored by the Financial Services Roundtable and BITS.

<http://www.identitytheftassistance.org/>

### **Identity Theft University - Business Partnership Michigan State University**

The partnership includes MSU researchers who are working with industry to make personal data more secure. This site includes information on technological, legal, psychological, and policy issues related to identity theft.

<http://www.cj.msu.edu/~outreach/identity/>

### **Internet Crime Complaint Center**

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

<http://www.ic3.gov>

### **International Association of Financial Crimes Investigators (IAFCI)**

IAFCI is comprised of public and private industry professionals who collectively work to prevent financial fraud worldwide.

1020 Suncast Lane, Suite 102  
El Dorado Hills, CA 95762  
Phone: (916) 939-5000  
Fax: (916) 939-0395  
<http://www.iafci.org/home.html>

### **National White Collar Crime Center (NW3C)**

A congressionally funded, non-profit corporation that equips state and local law enforcement agencies with skills and resources they need to tackle emerging economic and cyber crime problems through a combination of training and critical support services.

<http://www.nw3c.org>

### **Northwest License, Tax & Fraud Association**

Comprised of public and private employees, dedicated to the administration and enforcement of tax, license, and business registration laws, and to the detection, investigation, and prosecution of fraud.

Cindy Hubert  
President  
Pacific Northwest License Tax & Fraud Association  
P.O. Box 2291  
Seattle, WA 98111-2291  
Phone: (503) 454-3581  
<http://www.pnlfta.com>

**Eastern Massachusetts Compliance Network**

An association of 88 community bank compliance professionals, including compliance officers, attorneys and compliance auditors.

State Transportation Building  
10 Park Plaza, Suite 4510  
Boston, MA 02116  
Phone: (617) 973-8664

**NYCE Network Payments Advisory Council Meeting**

An electronic payments network that also provides research and white papers on topics of interest to financial institutions including fraud prevention, response, and recovery.

400 Plaza Dr.  
Secaucus, NJ 07094  
Phone: (201) 865-9000  
Fax: (201) 330-3374  
<http://www.nyce.net/index.jsp>

**Security of Fidelity National Information Services (FIS)**

FIS services range from core processing to e-banking, check imaging to business intelligence. Commercial banks, credit unions, and savings institutions use FIS services to improve their efficiency.

Diane Peterson  
United States Attorney's Office  
1000 SW 3rd Ave, Suite 600  
Portland, OR 87201

Phone: (503) 727-1066

Fax: (503) 727-1117

E-mail: [diane.peterson@usdoj.gov](mailto:diane.peterson@usdoj.gov)

### **Other Links and Resources**

#### **Avoiding Identity Theft**

The Pennsylvania Higher Education Assistance Agency (PHEAA) is a student loan guarantor. This resource provides information to students on how to protect themselves from identity theft.

E-mail: [info@ACFE.com](mailto:info@ACFE.com) (General inquiries)

<http://www.pheaa.org/tools/theft.shtml>

#### **Counterfeit Currency Awareness**

[http://www.secretservice.gov/know\\_your\\_money.shtml](http://www.secretservice.gov/know_your_money.shtml)

#### **How Identity Theft Works**

Describes how others can get access to personal identification information, how consumers can protect themselves, and what they can do if their information is stolen.

<http://www.computer.howstuffworks.com/identity-theft.htm>

#### **LLRX.com**

A free, independent, Web journal dedicated to providing legal, library, IT/IS, marketing and administrative professionals with the most up-to-date information on a wide range of Internet research and technology-related issues, applications, resources, and tools. The Web site contains a vast array of information from federal resources, federal laws, state resources, and recent GAO reports; selected CRS reports, consumer and industry resources, books, news articles, law review and law journal articles; and additional bibliographic information about identity theft.

Founder, editor, and publisher, Sabrina Pacifici is also the author of the current awareness fact blog on law and technology news, [www.bespacific.com](http://www.bespacific.com), which is updated daily.

<http://www.llrx.com/features/idtheft.htm>

**Privacy Rights Clearinghouse**

Fact sheets on identity theft in English and Spanish.

<http://www.privacyrights.org/identity.htm>

**University Resources on Identity Theft (from  
<http://connect.educause.edu>)**

Binghamton University:

<http://publicsafety.binghamton.edu/Identity%20Theft.htm>

Eastern Kentucky University:

<http://www.publicsafety.eku.edu/cp/identity.php>

University of Oklahoma:

<http://www.ou.edu/oupd/idtheft.htm>

University of Pennsylvania:

<http://www.upenn.edu/privacy/>

University of Rhode Island:

<http://www.uri.edu/admin/uripd/idTheft.php>



## APPENDIX C: CONTACT INFORMATION FOR SYMPOSIUM MEMBERS

### ***Project Participants***

Lester J. Bain  
VP/Investigation Manager, Chevy Chase Bank  
14601 Sweitzer Lane  
Laurel, MD 20707  
(301) 939-6604  
ljbain@chevychasebank.net

Jennifer Broadworth  
Officer/Fraud Supervisor, National City Bank  
Kalamazoo MI 49009  
(269) 973-1551  
jennifer.broadworth@nationalcity.com

Radha Chandra  
Risk Management Manager, Vice President  
Deposit Risk Analysis  
MAC A0103-140  
525 Market St, Suite 145  
San Francisco CA 94105  
(415) 547-3194  
radha.chandra@wellsfargo.com

Tanya Madison Cunningham, CIPP  
Counsel, First Data Debit Services  
1100 Carr Rd.  
Wilmington, DE 19809  
(302) 793-6034  
(302) 793-4423 (fax)  
tanya.madison.cunningham@firstdata.com

## WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT

---

Donald J. Devine, Jr.  
VP, Business Strategy Support & Risk Management  
First Data Debit Services  
1100 Carr Road  
Wilmington, DE 19809  
(302) 793-6015  
Don.Devine@FirstData.com  
www.FirstData.com  
www.Star.com

Scott Kelley  
Chief Investigator, Consumer Fraud and Economic Crime Division  
Office of Nola Tedesco Foulston, D.A.  
535 North Main St., 1st Floor Annex  
Wichita, KS 67203  
(316) 660-3648  
(316) 383-4638 (fax)  
skelley@sedgwick.gov

J. Patrick Lamb  
Birmingham Division  
Jefferson County District Attorney's Office  
801 Richard Arrington Blvd  
Birmingham, AL 35203  
(205) 325-5252  
lambp@jrhc.org

Sophia Lopez  
Supervisor, Consumer Fraud  
Cook County State's Attorney's Office  
69 W. Washington St., Room 930  
Chicago, IL 60602  
(312) 603-8641  
SLopez@cookcountygov.com

Camerino Mesina  
Vice President/Manager, Wells Fargo Bank  
Financial Crimes Investigations  
1050 Lakes Drive Suite 400  
West Covina, CA 91790  
(626) 919-6007  
Camerino.mesina@wellsfargo.com

Susan Storey  
Senior Deputy Prosecuting Attorney  
King County Prosecuting Attorney  
King County Administration Building  
Fraud Division  
500 Fourth Avenue, Room 840  
Seattle, WA 98104  
(206) 296-9010  
(206) 296-9009 (fax)  
susan.storey@metrokc.gov

Vincent Talucci  
Senior Program Manager, International Association of Chiefs of Police  
515 North Washington Street  
Alexandria, VA 22314  
(703) 836-6767, x-804  
talucci@theiacp.org  
www.idsafety.org

Sharon Werner  
Chief Attorney, Consumer Fraud and Economic Crime Division  
Office of Nola Tedesco Foulston, District Attorney  
535 North Main St., 1st Floor Annex  
Wichita, KS 67203  
(316) 660-3655  
(316) 383-4638 (fax)  
swerner@sedgwick.gov

## **WHO'S ON FIRST? CHALLENGES IN RESPONDING TO IDENTITY THEFT**

---

Frank E. White  
Assistant District Attorney, Consumer Fraud and Economic Crime  
Division  
Office of Nola Tedesco Foulston, District Attorney  
535 North Main Street  
Wichita, KS 67203  
(316) 660-3656  
(316) 383-4638 (fax)  
fwhite@sedgwick.gov

### ***Project Partners***

M. Elaine Nugent-Borakove  
Director, Office of Research and Evaluation  
National District Attorneys Association  
American Prosecutors Research Institute  
99 Canal Center Plaza, Suite 510  
Alexandria, VA 22314  
(703) 549-9222

Lisa M. Budzilowicz  
Research Analyst  
National District Attorneys Association  
American Prosecutors Research Institute  
99 Canal Center Plaza, Suite 510  
Alexandria, VA 22314  
(703) 549-9222

Kim Heavey  
SVP Security & Fraud  
First Data  
6200 S Quebec St.  
Greenwood Village, CO 80111  
(303) 967-7969  
kim.heavey@firstdata.com  
www.firstdata.com

## APPENDIX C: CONTACT INFORMATION FOR SYMPOSIUM MEMBERS

---

Kathryn Keefer  
Director, Strategic Marketing  
First Data  
6200 S Quebec St.  
Greenwood Village, CO 80111  
(303) 967-8251  
kathryn.keefe@firstdata.com  
www.firstdata.com