



APRI

American
Prosecutors
Research Institute

*If It Sounds Too
Good To Be True*

Local Prosecutors' Experiences
Fighting Telecommunications Fraud

American Prosecutors Research Institute

99 Canal Center Plaza, Suite 510

Alexandria, VA 22314

www.ndaa-apri.org

Thomas J. Charron

President

Debra Whitcomb

Acting Chief Administrator

George Ross

Director, Grants Management

This document was produced under Grant No. 98-LS-VX-0002 from the the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. This information is provided for educational purposes only and is not legal advice. Points of view or opinions expressed in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Justice, the National District Attorneys Association or the American Prosecutors Research Institute.

The American Prosecutors Research Institute is the nonprofit research, training and technical assistance affiliate of the National District Attorneys Association.

If It Sounds Too Good To Be True

Local Prosecutors' Experiences Fighting Telecommunications Fraud

September 2004

*James L. Johnson, Research Analyst,
Office of Research & Evaluation
Mark L. Miller, Deputy Director,
Office of Research & Evaluation
Stephanie Muller, Research Assistant,
Office of Research & Evaluation
Sean Morgan, Senior Attorney and Program Manager,
White Collar Crime Program
Patricia L. Fanflik, Senior Research Analyst,
Office of Research & Evaluation*

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314

TABLE OF CONTENTS

1	<i>Executive Summary</i>
3	<i>Introduction</i>
5	<i>Survey Results</i>
13	<i>Implications for Prosecutors</i>
15	<i>Glossary: Types of Telecommunications Fraud</i>
19	<i>Appendix A: Methodology and Sample Characteristics</i>
21	<i>Appendix B: Groups Prosecutors Regularly Work with in Combating Telecommunications Fraud</i>
23	<i>Resources</i>

EXECUTIVE SUMMARY

The advancement of technological tools such as computers, the Internet, and cellular phones has made life easier and more convenient for most people in our society. However, some individuals and groups have subverted these telecommunication devices into tools to defraud numerous unsuspecting victims. Local prosecutors are confronted with the challenge of gathering sufficient evidence to bring charges against suspects, a challenging task when it comes to telecommunications fraud. With new technology and increased criminal sophistication, many perpetrators are not only difficult to identify, they are even harder to locate.

This report summarizes a national survey of local prosecutors' offices, in which prosecutors were asked to identify challenges and barriers that arise in prosecuting telecommunications fraud cases as well as innovative and promising approaches they use to overcome those challenges.

According to more than 80 percent of the responding local prosecutors, credit card fraud and identity theft are the two most common forms of telecommunications fraud encountered by their offices, followed by:

- Internet auction scams (36 percent)
- ATM theft (35 percent)
- Theft of telecommunications services such as cell phone numbers (26 percent); and
- Fake solicitations for charitable donations (26 percent).

Findings from the American Prosecutors Research Institute's national survey indicate that local prosecutors are just beginning to scratch the surface in dealing with the complex issues that arise in cases of telecommunications fraud. The need for additional specialized training, information, and assistance is apparent. Less than 10 percent of offices with fewer than a half-million residents have a specialized prosecutorial unit that focuses on telecommunications fraud. Furthermore,

- Less than 20 percent of the offices indicate having established a multi-agency task force or formed partnerships with other agencies or organizations to handle telecommunications fraud complaints or investigations.
- A little more than 60 percent of prosecutors' offices indicated that their investigators and prosecutors do not have adequate training to handle telecommunications fraud cases.

As scams continue to increase in complexity, they require more time to investigate because identifying and locating perpetrators becomes substantially more difficult. It is not uncommon for a scam to originate in a city, county, state, or even country different from that in which the victim resides. This creates jurisdictional problems as well as logistical issues such as obtaining physical evidence and interviewing witnesses. Legal problems also arise, such as the appropriate legal process to obtain evidence outside the investigating agency's home jurisdiction. Based on APRI's survey, prosecutors consider the following challenges and barriers the most difficult to overcome:

- Time-consuming investigations (80 percent);
- Tracing financial transactions and documents (64 percent);
- Technological complexity of scams (53 percent);
- Identifying and locating perpetrators (50 percent); and
- Insufficient staffing (43 percent).

In addition, approximately one quarter of local prosecutors indicate that current statutes prevent them from obtaining evidence from Internet service providers (ISPs).

In addition to presenting findings from APRI's survey, this report also summarizes the types of information, skills, and materials prosecutors find most effective in combating telecommunications fraud.

INTRODUCTION

Society has made significant technological advancements over the past 30 years. Computers, the Internet, fax machines, cellular phones, and landline telephones are devices that have not only become vital necessities for businesses, but are also mainstays in our homes. The Internet gives us the ability to send messages worldwide in a matter of seconds, purchase merchandise ranging from books to computers to cars, and pay our monthly bills. Cell phones, which were once cumbersome and highly expensive, are now small enough to fit into a shirt pocket and inexpensive enough for nearly everyone to afford. Even the basic household telephone has made advancements to provide more conveniences. Cordless telephones have eliminated the burden of wrestling with tangled extension cords while granting increased range and mobility.

Technological advancement is, however, a double-edged sword; it creates opportunities while simultaneously producing consequences. Just as society is advancing and becoming more technologically sophisticated, so too are criminals. Although telecommunication tools make conducting business and routine tasks easier, they also make the business of fraud easier for con artists. New technologies are resulting in new ways to commit crimes against consumers.

Telecommunications fraud is a major concern for local prosecutors, law enforcement agencies, and consumers in general because nearly every household in America has at least one, if not several, telecommunication devices. This means that every household with a telephone, Internet service, or a fax machine has the potential of being solicited by con artists. No one is immune to telecommunications fraud. “Victims run the gamut of society,” states Chief Postal Inspector Lee R. Heath. “They’re wealthy, they’re poor, they’re old, [and] they’re young. Anyone can become a victim.”¹

The growth in telecommunications tools and services has fueled explosive growth in the types of frauds that are perpetrated on the unsuspecting. Con artists use electronic mail to distribute scams that, on the surface, appear to be legitimate business opportunities. Internet auction fraud, which is the fastest growing form of Internet fraud, bilks victims out of millions of dollars annually. Telemarketing fraud, the precursor to telecommunications fraud, continues to grow and cost consumers billions of dollars a year. No matter what the scam, criminals are a mere mouse click or telephone call away from defrauding people.²

When considering crime and crime victims, peoples’ thoughts generally focus on physical or violent crimes, such as armed robbery or rape. However, a University of Tennessee study found that more Americans become victims of fraud than of street crimes.³ In fact, fraudulent telemarketers victimize 100,000 Americans every week.⁴ Although

**“Victims run the
gamut of society.
They’re wealthy,
they’re poor, they’re old,
they’re young.
Anyone can become
a victim.”**
– *Chief Postal Inspector Lee Heath*

¹ U. S. Postal Inspection Services. (February 3, 2003). “Don’t give it away: Protect your good name from identity theft!” <http://www.usps.com/postalinspectors/nridthft.htm>. Retrieved August 25, 2003.

² Federal Trade Commission. “Dot Cons.” <http://www.ftc.gov/bcp/conline/pubs/online/dotcons.htm>. Retrieved September 4, 2003.

³ Jacobs, Don. (December 12, 2001). Telemarketing Con Artists Don’t See Selves as Criminals. *Scripps Howard News Service*.

⁴ “Telemarketing Fraud.” Available: <http://www.in.gov/attorneygeneral/consumer/telemarketingfraud.htm>. Retrieved September 4, 2003.

they suffer no physical injuries and perpetrators are never physically in their homes, victims of fraud feel the same anger, frustration, helplessness, and embarrassment experienced by victims of street crime. Victims also may experience a loss of independence, develop a more suspicious nature, or even come to question their own judgment.

Although rampant in society, telecommunications fraud is drastically underreported. The general consensus among government agencies and fraud experts is that most victims are just too embarrassed to report the crime. Many victims blame themselves, especially professional people who feel they “should have known better.” Still others are under the impression that their loss is too small to report or that law enforcement will not be able to do anything about the fraud.

On top of the emotional and psychological damage, financial losses (including money, property, and investments) can be devastating. Victims may be cajoled into mortgaging their homes or cashing in retirement accounts or their children’s college savings funds for an ostensibly sure thing. Additionally, victims may experience long-term credit problems as a result of these scams.

Telecommunications fraud is a widespread problem. Prosecutors report that these scams are becoming more complex, in part, because of available technology and sophistication of the criminals, jurisdictional issues, and the lack of resources and training necessary to successfully prosecute the increasing number of fraud cases.

Measuring State and Local Prosecutors’ Response

The American Prosecutors Research Institute (APRI) designed a survey and distributed it to state and local prosecutors in an effort to document current prosecutorial efforts in combating telecommunications fraud. For the purpose of this project, APRI defined telecommunications fraud as the use of telecommunication devices to intentionally deceive or criminally manipulate a person for financial gain. These devices include but are not limited to computers, computer networks, the Internet, fax machines, and telephones.

One of the main topic areas covered in the survey was challenges and barriers local prosecutors encounter when investigating and prosecuting telecommunications fraud cases. This nationwide survey also captured information on the following topics:

- Basic demographic information about the prosecutor’s office, including jurisdiction and office size;
- Whether the office has a specialized prosecutorial unit that addresses telecommunications fraud;
- The number of telecommunications fraud cases handled by the office;
- Most common forms of telecommunications fraud encountered in the office;
- Agencies the office regularly works with to combat telecommunications fraud;
- Activities engaged in (such as investigative, case management, law enforcement coordination, and outreach) with respect to telecommunications fraud;
- Statutory provisions regarding evidence obtainment; and
- Training topics of interest to respondents.

Although there are numerous variations of telecommunications fraud, this report will primarily highlight identity theft, Internet fraud, and telemarketing fraud. Many scams lurk under this typology including sweepstakes, credit repair, advanced fee loans, investment, and Internet auction fraud, just to name a few. The remainder of this report consists of three chapters. Results from the national survey will be presented first, followed by a description of implications of the survey results for prosecutorial practice. Finally, a glossary describes several prominent forms of telecommunications fraud.

SURVEY RESULTS

Telecommunications fraud is an evolving phenomenon—one that is becoming increasingly complex and is constantly changing to make use of new technology. As such, law enforcement and prosecutors are continually trying to “keep up.” These survey results shed light on where prosecutors currently are in terms of knowledge and skills regarding telecommunications fraud, and where they need to grow to more successfully address this ever-changing form of criminal activity.⁵

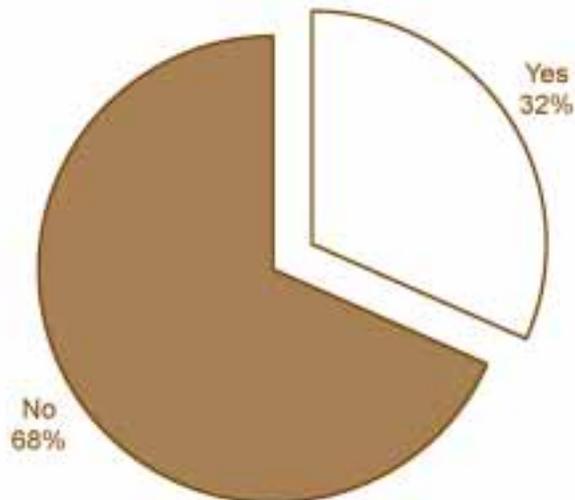
Office Characteristics

Offices that responded to the survey had a median⁶ staff of 20 full-time attorneys, 6 full-time investigators, and 21 other full-time staff. The majority of offices (68 percent) reported filing charges on one or more telecommunications fraud cases in the year preceding the survey. These offices also reported having a median of 2.5 prosecutors and less than 1 investigator to work on telecommunications fraud cases. During 2002, offices reported investigating, filing, and obtaining convictions on a median of 1 to 2 telecommunications fraud cases. Some offices, however, report processing dozens, even hundreds, of these cases. This shows that while *most* offices are prosecuting only a few of these types of cases, a handful of offices are prosecuting a great number of them. The remainder of this report will examine why this disparity exists.

Specialized Unit

As the scope of telecommunications fraud continues to expand, the need for specialized prosecutorial units that focus on this type of crime will become more apparent. Of the prosecutors who responded to the survey, 68 percent reported that their office did *not* have a specialized unit that included telecommunications fraud in its portfolio (Exhibit 1).

Exhibit 1
Office Has a Specialized Unit That Includes Telecommunications Fraud

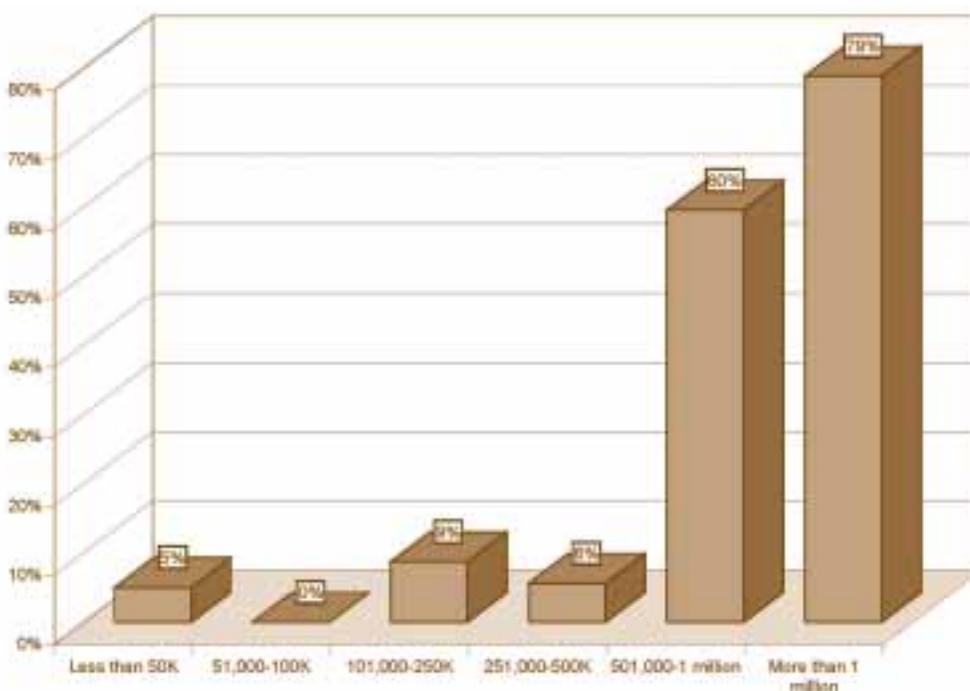


⁵ Appendix A provides information on the survey methodology and characteristics of the responding offices.

⁶ The median represents the score at the 50th percentile or midpoint of a distribution, which means that there are an equal number of cases above and below the median score. The median is better suited for skewed data (data with extremely high or low values) than the traditional mean (or average).

Smaller jurisdictions are less likely to have a specialized prosecutorial unit for telecommunications fraud than larger jurisdictions. Exhibit 2 illustrates that less than 5 percent of prosecutors' offices with fewer than 100,000 residents have created a specialized unit for telecommunications fraud. Prosecutors in jurisdictions with more than 1 million residents report the largest percentage of specialized units at 79 percent. Smaller jurisdictions are less likely to have specialized units because they typically have fewer prosecutors than larger jurisdictions and therefore cannot afford to specialize in a particular type of crime.

Exhibit 2
Percentage of Offices With a Specialized Unit That Includes Telecommunications Fraud By Population Size of Jurisdiction



How telecommunications fraud cases are assigned throughout prosecutors' offices can play an important role in combating these crimes. The survey revealed that local prosecutors use several approaches to case assignment:

- To a specialized unit (such as economic crimes) that includes telecommunications fraud cases as part of its mission (37 percent of responding offices);
- To attorneys with room on their caseloads (25 percent);
- To the next attorney in the case assignment rotation (20 percent); and
- To senior attorneys (12 percent).

Only 6 percent of the respondents assign these cases to an attorney with special expertise in telecommunications fraud.

After removing from the analysis those offices with a specialized unit, APRI learned that local prosecutors are most likely to assign telecommunications fraud cases to attorneys with room on their caseload (40 percent), followed by attorneys next in the case assignment rotation (33 percent). Together, these findings suggest that many local prosecutors are assigning telecommunications fraud cases to attorneys who may lack significant prior experience or training in such cases.

Common Forms of Telecommunications Fraud

Telecommunications fraud comes in a variety of forms. However, some scams are more prevalent than others. Surveyed prosecutors were asked to name the most common forms of telecommunications fraud they encounter. As revealed in Exhibit 3, the four most common forms of telecommunications fraud encountered by local prosecutors are credit card fraud, identity theft, internet auction scams, and ATM theft.

Exhibit 3
Most Common Forms of Telecommunications Fraud Encountered by Prosecutors

Forms of Telecommunications Fraud	Percentage of Cases
Credit card fraud	83
Identity theft	81
Internet auction scams	36
ATM theft	35
Fake solicitations (e.g., charities)	26
Theft of telecom services (e.g., theft of cell phone numbers)	26
Sweepstakes fraud	16
Advance fee loan scams	13
Computer hijacks (unauthorized computer access)	12
Prize promotions	12
Credit repair scams	10
Internet pyramid schemes	10
Electronic money laundering	8
Internet stock & investment frauds	8
Internet health/diet schemes	4
Magazine subscription fraud	4
Impersonation of bank/other officials	1
Other	6

Partnerships

By its very nature, telecommunications fraud crosses a variety of jurisdictional, geographical, and other boundaries. It follows, then, that to successfully combat telecommunications fraud, local prosecutors or the law enforcement agencies they work with need to establish task forces or partnerships with other agencies and organizations to gather evidence and identify witnesses, victims, and suspects. Despite this apparent need, only 18 percent of prosecutors' offices indicated forming such task forces or partnerships.

Larger jurisdictions are more likely to have formed partnerships than smaller jurisdictions. Only in the two largest population groupings have significant degrees of partnering transpired. For example, 58 percent of prosecutors in jurisdictions with more than a million residents enlisted the help of other agencies and organizations.

APRI asked local prosecutors to indicate, from a list of 34 groups, whom they regularly work with in combating telecommunications fraud. The results indicated that local prosecutors tend to work with a median of four different groups. Local police and sheriffs' departments are by far (76 percent) the group with whom local prosecutors are most likely to work. Also listed by at least 40 percent of the surveyed prosecutors were the state attorney general, the state police agency, and the U.S. Postal Service. (Although mail fraud is not a form of telecommunications fraud, many telemarketing and Internet scams are hybrids of such schemes, which may explain why local prosecutors so frequently reported working with the U.S. Postal Service.)

Prosecutors did not limit the groups they work with to law enforcement agencies. For example, 28 percent of local prosecutors report teaming with financial institutions, while 25 percent work with telecommunication companies. This tendency to seek out partners from agencies other than law enforcement did not vary by the size of the jurisdiction: It was as likely to occur in small jurisdictions as it was in large jurisdictions.

Challenges

According to survey results, 67 percent of prosecutors reported *no* change over time in the difficulty of investigating and prosecuting telecommunications fraud cases. However, among those prosecutors (31 percent) who indicated investigating and prosecuting these cases *had grown more difficult*, improved technology and greater criminal sophistication were the primary challenges they faced. Other significant reasons for the increased difficulty in handling telecommunications fraud cases included multi-jurisdictional issues; lack of resources; lack of cooperation from telecommunication companies, victims, and federal agencies; and challenges in identifying and locating perpetrators.

APRI expected that as the size of a jurisdiction increased, so too would the difficulty in investigating and prosecuting these cases. (The scams would also increase in quantity as well as in complexity in larger jurisdictions.) The survey results generally reflect this prediction. In the two largest jurisdiction categories, more than 40 percent (47 percent and 41 percent respectively) of prosecutors consider telecommunications fraud cases more difficult to investigate and prosecute than they once were. Unexpectedly, prosecutors in jurisdictions with fewer than 250,000 residents were roughly twice as likely (or more) to report telecommunications fraud cases being more difficult to investigate and prosecute than were prosecutors working in jurisdictions with from one quarter to a half million residents. It may be that for smaller jurisdictions, the scams themselves may not be more complex, but resource constraints may be increasingly limiting the abilities of prosecutors to fight these crimes.

Another potential challenge for local prosecutors is the degree to which judges understand telecommunications fraud crimes and view them as important. Nearly half of responding prosecutors' offices found that judges in their jurisdictions did not understand telecommunications fraud crimes (11 percent), did not view them as important (22 percent), or both (12 percent). The remaining respondents felt that judges in their jurisdictions both understand telecommunications fraud crimes *and* view them as important. Understanding and appreciation of telecommunications fraud crimes among the judiciary is a critical factor because judicial approval of legal processes and the resources needed to investigate cases is often required.

Barriers

Prosecuting telecommunications fraud is a daunting task for nearly all prosecutors. Computers and the Internet have allowed many criminals to execute scams thousands of miles from where their victims reside. "Crime scenes" typically

lack a substantial amount of physical evidence. Phony e-mail accounts can direct investigators to numerous dead ends. Therefore, it is not surprising to see in Exhibit 4 that 80 percent of local prosecutors declared the time-consuming nature of investigations as one of the biggest problems they face in combating telecommunications fraud. Difficulty in tracing financial transactions/documents was reported by more than 60 percent of prosecutors, while roughly half of the respondents identified the technological complexity of the crime and locating scammers as problems.

Exhibit 4
Most Difficult Problems Faced by Local Prosecutors
When Combating Telecommunications Fraud

Types of Problems	Percentage of Cases
Time-consuming nature of investigations	80
Tracing financial transactions/documents	64
Technological complexity of crimes	53
Identifying location of scammers	50
Insufficient staffing	43
Lack of expertise	36
Lack of cooperation from intermediaries (e.g., financial services)	33
Evidentiary issues	32
Losses too small to pursue	24
Reaching out to and educating potential victims	18
Poor coordination among interested groups	17
Lack of training opportunities	16
High numbers of scams in operation	15
Lack of cooperation by law enforcement in other jurisdictions	15
Victims unwilling/unable to participate	11
Getting referrals	10
Lack of victim services	10
Other	10

Typically, crimes are prosecuted in the jurisdiction in which the crime was committed, but the Internet and other telecommunication devices have in essence created two crime scenes: one where the bait was cast and the other where the victim was hooked. Identifying perpetrators is a monumental task for prosecutors, but knowing their location makes the task a little easier. According to the survey:

- 63 percent of the prosecutors state that perpetrators are typically located within their jurisdiction;
- 8 percent said that the offenders were outside their jurisdiction but within their state;
- Another 25 percent of the respondents reported that perpetrators were located outside of their state, but within the United States; and
- Only 4 percent of prosecutors stated that scammers were outside the United States.

The survey suggests that current statutes are not one of the barriers to prosecuting telecommunications fraud cases. Of the surveyed prosecutors, 75 percent indicated that statutes governing obtaining electronic evidence from ISPs do *not* prevent them from pursuing telecommunications fraud investigations. Likewise, 74.5 percent of the respondents felt that current statutes pertaining to confiscating financial or ISP records do *not* inhibit investigations.

Of the prosecutors who felt that statutes were problematic, many suggested the statutes be changed so that subpoenas and warrants on ISPs would apply across jurisdictions. Apparently, out-of-state subpoenas have been refused by jurisdictions that did not issue the subpoena or warrant. Some prosecutors would also like to have increased and easier access to ISPs and other records. Essentially, prosecutors would like to eliminate some of the red tape involved in obtaining search warrants for ISPs and broaden the scope of information they can access. Another suggested improvement is better record keeping, including extending the length of time ISP records are retained.

Victims

While senior citizens are believed to be the most frequent targets of scam artists, results from the national survey provided mixed support for this belief. According to 64 percent of surveyed prosecutors, no particular age group is targeted more frequently in their jurisdiction. On the other hand, among those prosecutors who felt an age group was targeted more often, 65 percent reported that individuals age 65 years or older were targeted with greater frequency.

Prosecutor offices were split nearly fifty-fifty when asked whether a particular age group suffered a more severe impact from telecommunications fraud. For prosecutors who thought there was a difference in the amount of suffering, there was overwhelming sentiment (84 percent) that people who are 65 years or older suffer the greatest impact.

Prosecutor Activities Related to Telecommunications Fraud

Combating a seemingly faceless crime such as telecommunications fraud can require prosecutors to engage in a multitude of activities ranging from investigation to community outreach. APRI asked local prosecutors to identify which, of 15 possible investigative, case management, law enforcement coordination/cooperation, and consumer education/outreach activities they frequently engage in.

As shown by Exhibit 5, getting search warrants for electronic or computer-based evidence and obtaining evidence from ISPs were listed by from 60 to 80 percent of the prosecutors.

Exhibit 5
Activities Engaged in by Local Prosecutors
to Combat Telecommunications Fraud

Investigative Activities	Percentage of Cases
Search warrants for electronic or computer-based evidence	79
Obtaining evidence from Internet Service Providers	59
Wiretaps	11
Search warrants/administrative searches of Call Centers	11
Case Management Activities	
Provision of services to victims	54
Developing tools to recognize and investigate cases	21
Developing standard forms and reporting procedures	18
Creating databases & other tracking tools	11
Law Enforcement Coordination/Cooperation Activities	
Training law enforcement organizations	31
Hosting conferences/meetings	19
Consumer Education/Outreach Activities	
Training community groups or financial institutions	27
Public awareness campaigns	23
Developing informational or educational materials/brochures	14
Developing informational or educational websites	8
Other	3

Of the case management activities, more than half of the surveyed prosecutors indicated providing services to victims, while a fifth have developed tools to help in the recognition and investigation of telecommunications fraud crimes. Staying abreast of current trends, laws, and fraudulent schemes is essential not only for prosecutors, but also for law enforcement and consumers. Thus, 31 percent of responding prosecutors conduct trainings for law enforcement organizations. Roughly a quarter of the prosecutors also participate in public awareness campaigns and conduct trainings for community groups, which may include personnel from financial institutions.

Training Needs

The survey revealed that 61 percent of the local prosecutors' offices report that investigators and prosecutors in the office do not have adequate training to handle telecommunications fraud cases. Overall, surveyed offices attended a total of 113 trainings during the prior year, which averages out as less than one training per office for the year. Fifty-two percent of the offices reported not attending any trainings.

There was a striking contrast between prosecutors’ offices that felt they were adequately trained to handle telecommunications fraud cases versus those that did not feel adequately trained. Of the local prosecutors’ offices that claimed to be adequately trained, 28 percent attended only one training in the past year, while more than 40 percent attended two or more trainings. Conversely, 61 percent of offices that did not feel adequately trained did not attend a single training during the past year while 32 percent attended only one. None of the inadequately trained offices attended more than three trainings during the past year.

To better understand the training needs of local prosecutors, APRI asked the respondents to indicate which, among 12 content areas, would be of interest to individuals in the office. Exhibit 6 shows that the four leading areas were computer technology as it applies to telecommunications fraud, search and seizure laws for electronic evidence, how to deal with frauds involving multiple jurisdictions, and how to introduce electronic evidence in court. Each of these was endorsed by at least 60 percent of the surveyed prosecutors.

Exhibit 6
Training Content Areas of Interest for Local Prosecutors

Training Content Areas	Percentage of cases
Search and seizure laws for electronic evidence	70
Computer technology relevant to TELECOM fraud	71
Dealing with cases involving multiple jurisdictions	66
Introducing electronic evidence in court	62
Role of financial institutions	56
Evidence collection and preservation	54
Special investigative techniques	54
Use of disposable technology (e.g., cell phones, calling cards)	44
Wiretapping issues	28
Working with victims from special populations (e.g., the elderly)	17
Civil law relevant to TELECOM fraud	13
Other	3

IMPLICATIONS FOR PROSECUTORS

Technological advancements have created new opportunities for criminals to defraud consumers. Although some aspects of modern telecommunication scams are no different from scams of yesteryear, the instruments used to commit these frauds pose challenges and barriers that were not present in the past. Prosecutors were not concerned with search and seizure laws for electronic evidence, nor did they ponder how to introduce evidence from an ISP into court 20 years ago. Today, these are common challenges in telecommunications fraud cases. These survey results demonstrate the three major challenges facing prosecutors in combating telecommunications fraud—the needs for specialization, partnership, and training.

Specialization

APRI's national survey revealed that the majority of prosecutors' offices did not have specialized prosecutorial units that focused on telecommunications fraud cases. Prosecutors' offices that investigate more than a handful of telecommunications fraud cases annually may wish to consider creating a specialized unit or designating a specific prosecutor for enhanced training to handle these cases. Prosecuting telecommunications fraud requires specialized knowledge of search and seizure laws, the Electronic Communications Privacy Act, financial privacy laws, and how best to present these cases to a judge or jury. Knowledge of computers, electronic evidence, disposable technology, and multi-jurisdictional issues are all required to effectively investigate and prosecute telecommunications fraud cases. Frequently, investigators will need guidance from prosecutors to avoid running afoul of the complex case law and statutes governing search and seizure of electronic evidence. Prosecutors must be trained to provide this assistance.

As local prosecutors improve their overall knowledge of these crimes and become more familiar with laws and procedures regarding electronic evidence, the amount of time spent tracing financial transactions and locating scammers should decrease.

Partnerships

Less than one-fifth of the surveyed prosecutors' offices have chosen to create a task force or establish partnerships with outside agencies to improve the response to telecommunications fraud. Collaborations with both public and private sector agencies is essential, and especially so for smaller jurisdictions. Prosecutors need to partner with diverse groups with expertise in the business world, such as financial institutions, as well as regulatory agencies like the Federal Trade Commission (FTC) to overcome the jurisdictional and logistical issues often posed by these cases. Local prosecutors can facilitate such partnerships by establishing relationships with these groups and developing procedures for attacking telecommunications fraud cases collectively. Even informal relationships, such as monthly or bi-monthly roundtable meetings, can help to ensure that agencies are not duplicating investigations, as well as serve to increase cooperation and information sharing.

Victim Assistance and Community Outreach

More than half (54 percent) of the respondents indicated that they provide assistance to telecommunications fraud victims. Regardless of whether these scams are aimed at older persons, respondents overwhelmingly agreed that persons over 65 are impacted the most by telecommunications fraud. Prosecutors should at least be able to inform victims regarding assistance resources. Such assistance can help ameliorate the loss to the victim, encourage further reporting of these crimes, and prevent the victim from being re-victimized. Potential resources may include the FTC's Consumer Sentinel, adult protective services, or friends and family of the victim.

Community outreach is another underutilized strategy to address telecommunications fraud. The old saw of “an ounce of prevention is worth a pound of cure” certainly holds true in telecommunications fraud. Only approximately a quarter of the respondent offices reported either training community groups or conducting public awareness campaigns relating to telecommunications fraud. Because of the time-consuming nature of these cases, if community outreach can prevent even a few persons from being victimized, the effect on law enforcement resources can be very beneficial. Possible community outreach strategies include a fraud alert system, public service announcements released to the media, and training community groups about on-line and telephone safety.

Training Needs

More than 60 percent of surveyed prosecutors indicated that their offices did not have adequate training to handle telecommunications fraud cases. Without adequate training, prosecutors are less likely to pursue telecommunications fraud cases because they are unsure of how to deal with the complexities and nuances associated with this type of crime. The more prosecutors learn about the various scams, current trends, computer technology relevant to telecommunications fraud, and laws related to electronic evidence, the more likely they will be able to successfully investigate and prosecute these crimes.

Database Management

Compiling telecommunications fraud incidents into a searchable database can be an extremely useful investigative tool. Unfortunately, only 11 percent of prosecutors’ offices surveyed answered that they had created such a database. Telecommunications fraud scams (many of which are described in the Glossary) are premised upon reaching large numbers of people in a low-cost, difficult-to-trace manner. This generally means that these fraudsters rely upon the telephone, email or websites to pitch the scam to victims. It is a “bulk” approach to perpetrating crime. With a database, investigators can see if a scam with similar characteristics has been reported within the jurisdiction and also respond to inquiries from other jurisdictions. Such a database can be particularly valuable where a jurisdiction contains a number of law enforcement agencies. This type of information mining and sharing can help develop a case and assist prosecutors in proving fraudulent intent beyond a reasonable doubt. Investigators and prosecutors also should avail themselves of two law enforcement-only consumer fraud databases, the FBI’s Internet Fraud Complaint Center and FTC’s Consumer Sentinel.

Finally, by establishing formal data collection procedures to document the number and types of cases investigated, prosecuted, and disposed of, prosecutors can begin to gather accurate information on the extent of telecommunications fraud. Such information would be valuable to policymakers, community groups, funding agencies, and others.

GLOSSARY: TYPES OF TELECOMMUNICATIONS FRAUD

Identity Theft

■ Identity theft involves “the misuse of information that is specific to an individual in order to convince others that the imposter is the individual, effectively passing oneself off as someone else.”⁷ Federal law defines identity theft as when a person “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law.”⁸ State laws sometimes require a fraudulent purpose or intent. There are a variety of ways in which an identity thief can gain access to a target’s personal information:

- Steal the victim’s wallet or purse, which usually contains identifying information such as driver’s licenses, credit cards, social security cards, and bankcards;
- Rummage through a person’s trash or the dumpster for an apartment building or business to obtain transaction receipts (a practice known as dumpster diving);
- Use a special information storage device to secretly copy the magnetic strip on the back of credit and debit cards during a normal transaction such as an ATM withdrawal or in-store purchase (this is called skimming);
- Pose as legitimate businesses by creating e-mail and Web site addresses to encourage individuals to provide credit or debit card account numbers (a technique referred to as phishing); and
- Insider schemes where the identity thief purchases personal information, from a person with legitimate access to information.

Financial fraud. Financial fraud is the most prevalent form of identity theft. This type of identity theft includes using another person’s identity for the purpose of:

- Opening a bank account;
- Opening new credit card accounts;
- Establishing wireless phone service;
- Committing computer fraud;
- Committing social program fraud (e.g., social security or welfare);
- Filing fake tax statements to obtain fraudulent returns; or
- Filing a change of address to intercept credit card bills.

Criminal activities. This type of identity theft involves taking on someone else’s identity in order to commit a crime. These criminal activities can include:

- Entering a country illegally;
- Getting special permits (e.g., work visas);
- Hiding one’s own identity;
- Committing acts of terrorism;
- Computer and cyber crimes;
- Alien smuggling; and
- Money laundering.

⁷ Finch, Emily. (2003). What a Tangled Web We Weave: Identity Theft and the Internet. In Yvonne Jewkes (ed.), *Dot.cons: Crime, Deviance, and Identity on The Internet* (pp. 86-104). Portland, OR: Willan Publishing

⁸ Identity Theft and Assumption Deterrence Act of 1998. Available: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=publ318.105. Retrieved September 3, 2003.

Internet Fraud

Internet fraud refers to “any type of fraud scheme that uses one or more components of the Internet—such as chat rooms, e-mail, message boards, or Web sites—to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.”⁹ There are a variety of Internet frauds:

Auction and Retail Schemes. These schemes typically attract consumers by purporting to offer high-value merchandise ranging from expensive jewelry to computers to sports memorabilia at very attractive prices. After persuading victims to send money in the form of a personal check, money order, or cashier’s check, schemers either send an inferior item or nothing at all.

Nigerian Money Offer Scams (or 419 Scams). Potential victims receive, either through e-mail or fax, a request from a purported high-ranking Nigerian government official (with the title of Doctor, Chief, or General) seeking permission to transfer a large sum of money (generally millions of U.S. dollars) out of Nigeria or some other African country into the victim’s bank account. In exchange, victims are promised a percentage of the money, usually 20 to 30 percent. To consummate the deal, victims only need to send their bank information, business letterhead, and telephone and fax numbers to the government official. After providing the requested information and before receiving the money, victims are extorted to pay money to overcome an endless number of unforeseen financial hurdles such as handling and processing fees or lawyer fees.

Business Opportunity/Work-at-Home Schemes. Typical business opportunity/work-at-home ads promise a “large income” for working on projects “in great demand.” While perhaps making available official-looking documents and materials (such as brochures or reference lists), many of these scams fail to disclose hidden costs such as placing newspaper ads; photocopying materials; or buying envelopes, stamps, paper, and other supplies or equipment necessary to complete the job. The ads also omit the fact that you may have to work many hours before receiving any pay. Some companies sponsoring the ads may also demand that their victims pay for instructions or “tutorial” software.¹⁰ The one characteristic common to all of these schemes is that victims are required to purchase something before they are able to start work.

Examples of classic work-at-home schemes include the following:

Medical billing. For an investment of \$2,000 to \$8,000, an advertiser will promise software, training and technical support so investors can provide services such as billing, accounts receivable, electronic insurance claim processing, and practice management to doctors and dentists. Consumers quickly find out that there is no market for their line of business and are unable to secure clients.

Envelope stuffing. This scam is predicated on getting individuals to pay a small start-up or registration fee, typically from \$19.95 to \$49.95, to learn how to earn extra money stuffing envelopes. Unfortunately, modern technology has rendered stuffing envelopes by hand virtually obsolete. For their registration fee, opportunity seekers receive instructions on how to defraud others by advertising the same envelope stuffing scam in newspapers, magazines, or websites.

Assembly or craftwork. Advertisers solicit individuals to assemble or to make products such as toys, jewelry, baby booties, or plastic signs at home. In order to make the products, individuals must spend hundreds of dollars

⁹ U.S. Department of Justice. (2001). “Internet Fraud.” Available: <http://www.usdoj.gov/criminal/fraud/text/Internet.htm>. Retrieved September 10, 2003.

¹⁰ Federal Trade Commission. (March 2001). “Work-at-Home Schemes.” Available: http://www.pueblo.gsa.gov/cic_text/employ/workathome/home.htm. Retrieved September 23, 2003.

to purchase a kit with the requisite instructions, materials, and equipment. The company promises to buy those items that meet their requirements. Seldom do any of the finished products meet the company's "standards" and the products are nearly impossible to sell.

Investment Schemes. Market manipulation scams are at the forefront of this type of scheme. There are basically two methods employed in manipulating the market. The first method, commonly known as the pump-and-dump, attempts to drive up the price of thinly traded stocks or stocks of shell companies by sending out e-mails that inflate the value of the company. When new purchases of the stock push its price to a high enough level, the scammers sell off their stock to realize a significant return, which in turn drives down the stock price and wipes out the investments of the people who had been duped. The second method, referred to as short-selling or scalping, tries to decrease a stock's value.

Telemarketing Fraud

Telemarketing fraud refers to "any scheme to defraud in which the persons carrying out the scheme use the telephone as their primary means of communicating with prospective victims and trying to persuade them to send money to the scheme."¹¹ These schemes include but are not limited to soliciting a person to buy goods and services, to invest money, or to donate funds to charitable causes. Individuals are typically targeted by would-be scammers purchasing from legitimate organizations' "mooch lists" containing personal information (e.g., names, phone numbers), or by scouring obituary pages for surviving spouses of senior citizens.

Advanced Fee Loans. Consumers receive a call almost guaranteeing that, regardless of past credit history, they will be approved for a loan to cover outstanding bills or debts. All the consumer has to do is pay an advanced fee. Once credit card information has been given, or cash received, the lender either informs the victims that their loan applications have been denied or, more frequently, is never heard from again.

Credit Card Offers. Unsuspecting consumers make easy prey for this ruse if their income or credit history is such that they are not eligible for a legitimate credit card. Once an initial required fee is paid, another payment may be required and the credit limit may not exceed the rendered payment amount. In essence, the consumer has paid for the privilege to use his or her own money. In other cases, after the initial fee is paid, no card is ever received.

Many credit card holders receive offers for credit card protection. The caller tries to convince the cardholder that additional protection/insurance is necessary to guard against unauthorized charges. The FTC warns against any purchase of additional credit card protection because consumers are only liable for \$50 in unauthorized charges if they follow the credit card company's procedures for dealing with such charges.¹²

Sweepstakes/Prize Offers. In the contemporary version of sweepstakes/prize offer schemes, consumers are told that they have won one of five valuable prizes, ranging from a new car to thousands of dollars in cash to expensive jewelry. After paying a fee or buying a required product, the victim receives a gimmie gift, which is often some cheap jewelry or other worthless trinket. The item received costs the telemarketer a mere fraction of the amount the victim paid out.

Magazine Subscriptions. Magazine subscription scams work in much the same way as the sweepstakes scam, except victims are required to buy multiple magazine subscriptions in order to receive their prizes. The magazines

¹¹ U.S. Department of Justice. "What Is Telemarketing Fraud?" Available: <http://www.usdoj.gov/criminal/fraud/telemarketing/whatis.htm>. Retrieved September 4, 2003.

¹² Federal Trade Commission. "Ditch the Pitch: Hanging Up on Telephone Hucksters." Available: <http://www.ftc.gov/bcp/online/pubs/tmarkg/ditch.pdf>. Retrieved September 4, 2003.

purchased are either not provided or provided only in part. The telemarketers may encourage participation by insisting that they are “just like” a nationally known and legitimate organization.

Vacation Offers. In these scams, a vacation package is purchased cheaply by a company which in turn collects several times its value in “taxes and fees” from the victim. In one particular instance, after having paid nearly \$250 in necessary fees and taxes on their “free” vacation prize, the victims were disappointed to discover that the vouchers they received for their one-week vacation package didn’t include airfare, ground transportation costs, food, or other costs. There were also restrictions on the vouchers.¹³

Recovery room schemes. After victims have lost money to a particular scam or string of scams, a follow-up recovery room scheme is ready to further defraud them. Pretending to be working with some law enforcement agency, government office, the local prosecutor’s office or the local courts, a telemarketer connected to the original artifice will contact the victim under the pretense of wanting to assist in recovering some of their losses. Due to previous involvement, schemers have inside information in terms of the extent of financial losses as well as how the losses occurred. To complete the ruse, victims are asked to send more money in order to recoup their original losses.¹⁴

Rip and tear schemes. These schemes are not necessarily scams in and of themselves, but can more accurately be described as a modus operandum. Rip and tear telemarketers concentrate on moving around and not leaving a paper trail. They make calls from a variety of phones, commonly using pay phones, cloned cell phones, or pre-paid cell phones, all of which are difficult to trace. Collecting traceless payments requires the use of commercial mailbox services (rented under an alias), electronic wire transfers, and even the use of a middleman.¹⁵ Further complicating the investigation, perpetrators often contact victims who live in different states and even different countries, introducing jurisdictional issues.

¹³ Henderson, Les. “Crimes of Persuasion—Schemes, Scams, Frauds.” Available: <http://www.enovel.com/sample.html?p=7443>. Retrieved September 5, 2003.

¹⁴ U.S. Department of Justice. “What Kinds of Telemarketing Schemes Are Out There?” Available: <http://www.usdoj.gov/criminal/fraud/telemarketing/schemes.htm>. Retrieved September 4, 2003.

¹⁵ *Ibid*

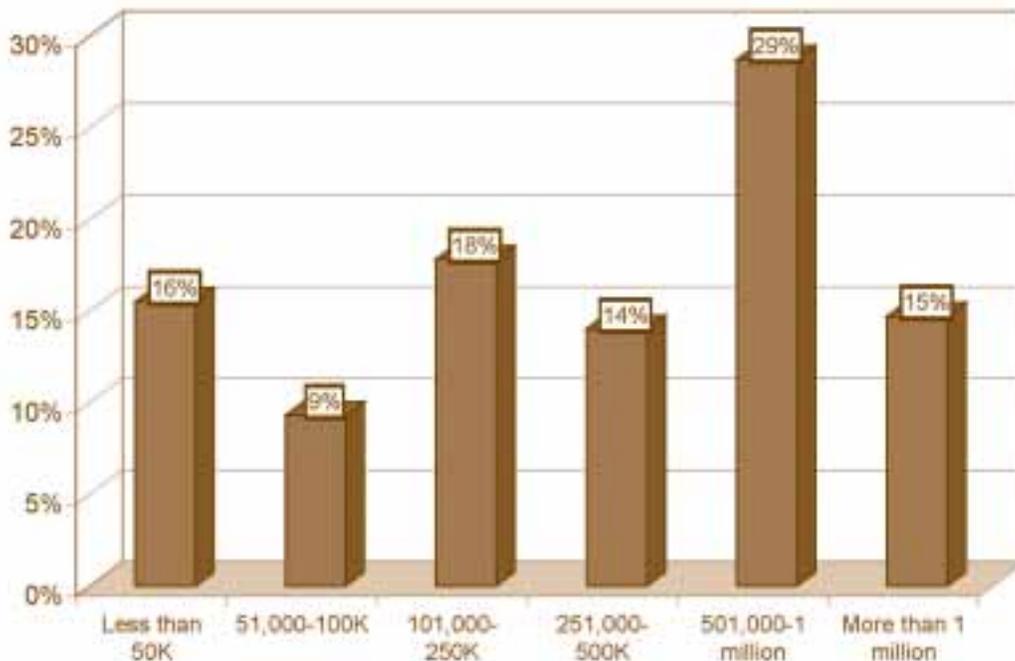
APPENDIX A: METHODOLOGY AND SAMPLE CHARACTERISTICS

A nationally representative sample of 310 local prosecutors' offices received APRI's telecommunications fraud survey during June and July of 2003. Prosecutors first received the survey via fax or e-mail in the month of June and were given 14 days to complete it. APRI conducted telephone follow-ups to prosecutors' offices located in jurisdictions with a million or more residents that failed to complete the survey by the initial deadline. All offices that failed to complete the initial survey were faxed another copy of the survey. These offices were given an additional 10 days to complete the survey. Overall, prosecutors from 129 offices in 40 different states responded to the survey, providing a response rate of nearly 42 percent.

The primary objective of the survey was to document local prosecutors' experiences with telecommunications fraud. These experiences included challenges and barriers faced when investigating and prosecuting these crimes; investigative and case management activities; the use of task forces or partnerships; and the most common forms of telecommunications fraud encountered.

The survey also collected basic demographic information such as size of jurisdiction and office characteristics, particularly number of attorneys, investigators, and other staff members. Jurisdictions of varying sizes responded to the survey. Exhibit 7 highlights the survey respondents by jurisdiction size. The greatest percentage of responses came from prosecutors in jurisdictions with 501,000 to 1 million inhabitants (29 percent). Of the 129 responding jurisdictions, 18 percent had populations of 101,000 to 250,000. The remaining jurisdictions represented between 9 percent (51,000 to 100,000) and 16 percent (less than 50,000) of the population surveyed.

Exhibit 7
Percentage of Survey Respondents by Jurisdiction Size



IF IT SOUNDS TOO GOOD TO BE TRUE

Responding jurisdictions were distributed throughout the four main regions of the country. The South was represented most often, as 33 percent of the responding offices were located in southern states. Both the Midwest and the East were responsible for 24 percent of the surveyed jurisdictions, followed by the North with 19 percent of the returned surveys.

APPENDIX B:

GROUPS PROSECUTORS REGULARLY WORK WITH IN COMBATING TELECOMMUNICATIONS FRAUD

FEDERAL LAW ENFORCEMENT AGENCIES	Pct. of cases
Federal Bureau of Investigation	39
U.S. Postal Service	40
U.S. Secret Service	25
U.S. Customs	8
Internal Revenue Service	7
Securities and Exchange Commission	4
U.S. Attorney's Office	25
Social Security Administration	6
Other federal law enforcement agency	4
STATE REGULATORY AND SOCIAL SERVICES AGENCIES	
Department of State	3
Area Agencies on Aging	6
Adult Protective Services	10
Other State Regulatory/Social Service Agency	13
FEDERAL REGULATORY AGENCIES	
Federal Trade Commission	7
Federal Communications Commission	2
Other Federal Regulatory Agency	1
STATE LAW ENFORCEMENT AGENCIES	
State Police Department	43
State Attorney General	45
State Bureau of Investigation	17
Other State Law Enforcement Agencies	12
LOCAL LAW ENFORCEMENT AGENCIES	
Local Police/Sheriff's Depts.	76
TRIAD/SALT	5
PRIVATE SECTOR ORGANIZATIONS	
Telecommunications Companies	25
Financial Institutions	28

continued

Media (e.g., newspapers, TV)	9
Medical Providers/Hospitals	2
Care/Living Facilities	4
Other Private Sector Organizations	6
PUBLIC INTEREST ORGANIZATIONS	
Senior Citizen Groups (e.g., AARP)	10
Consumer Groups/Bureau	6
Civic Groups/Clubs	4
Faith Community	1
Other Public Interest Organizations	3

RESOURCES

Technical Assistance

American Prosecutors Research Institute

99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
(703) 549-4253
www.ndaa-apri.org

APRI Contacts

Sean Morgan

Senior Attorney and Program Manager,
White Collar Crime Program
(703) 519-1666

Additional Contacts

American Association of Retired Persons

601 E. Street, NW
Washington, DC 20049
(800) 424-3410
(202) 434-2277
www.aarp.org

Bureau of Justice Assistance

810 Seventh Street NW,
Fourth Floor
Washington, DC 20531
(202) 616-6500
www.ojp.usdoj.gov/BJA

Bureau of Justice Statistics

810 Seventh Street, NW
Washington, DC 20531
(202) 307-0765
www.ojp.usdoj.gov/bjs

Consumer Sentinel

Consumer Sentinel Project Team
600 Pennsylvania Avenue NW
Washington, DC 20580
E-mail: sentinel@ftc.gov
www.consumer.gov/sentinel

Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

National District Attorneys Association

99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
(703) 549-4253
www.ndaa-apri.org

National Fraud Information Center

P.O. Box 65868
Washington, DC 20035
(800) 876-7060
www.fraud.org

National Institute of Justice

810 Seventh St., NW
Washington, DC 20531
(202) 307-2942
www.ojp.usdoj.gov/nij

U.S. Department of Justice

U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
(202) 514-2008
www.usdoj.gov

APRI Publications

- *Telemarketing Fraud Prevention and Prosecution: The Experience of Five Demonstration Sites*
- *Telemarketing Fraud Investigation, Prosecution and Prevention Manual and Video*
- *Secure Lines (CD)*

