SPECIAL TOPICS SERIES

APRI

American
Prosecutors
Research Institute

21st Century Phraud

Three Jurisdictions' Efforts to Combat Telecommunications Fraud

BJA Bureau of Justice Assistance

Office of Justice Programs • U.S. Department of Justice

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314
www.ndaa-apri.org

Thomas J. Charron
President

Roger Floren
Chief of Staff

Sean Morgan
Program Manager, White Collar Crime Program

Debra Whitcomb
Director, Grant Programs and Development

George Ross
Director, Grants Management

This document was produced under Grant No. 98-LS-VX-0002 from the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. This information is offered 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 United States Department of Justice, the National District Attorneys Association, the American Prosecutors Research Institute, AARP, the National Association of Attorneys General, or the National White Collar Crime Center.

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

21st Century Phraud

Three Jurisdictions' Efforts to Combat Telecommunications Fraud

April 2005

Sean Morgan
White Collar Crime Program Manager
American Prosecutors Research Institute

James Johnson
Research Analyst
American Prosecutors Research Institute

TABLE OF CONTENTS

INTRODUCTION

Fraud using the Internet and telephone lines is a multi-billion dollar "enterprise" that victimizes hundreds of thousands of consumers annually and indirectly affects our entire society by causing a loss of confidence in the e-commerce economy of the 21st century. These telecommunications fraud scams present unique problems to local law enforcement and prosecutors because the scams are typically multi-jurisdictional, i.e., the perpetrator located in one jurisdiction uses the Internet or the telephone to convey the fraudulent misrepresentation to the victim, who is located in another jurisdiction. To complicate matters further, the fraudster often will send the money obtained through these false representations to yet a third location in another jurisdiction.

Local law enforcement and prosecutors, if they are in the victim's jurisdiction, are then in a position of having to investigate a crime where most of the evidence and the perpetrator are located elsewhere. If the local law enforcement and prosecutors are in the perpetrator's jurisdiction, they are in the position of having to expend precious resources in manpower and money to prosecute a crime when no one within their jurisdiction is victimized. If local law enforcement and prosecutors have jurisdiction over the money drop location, they have only some of the evidence and neither the victim nor perpetrator.

The effect of these jurisdictional issues is compounded by several other factors. First, telecommunications fraud scams are typically a "volume" business with tens—even hundreds—of victims residing in different jurisdictions or even if located within the same prosecutorial district not within the same local police agency jurisdiction. Second, demonstrating the intent to defraud in these scams often requires investigating and obtaining evidence on all or many of the incidents generated by a single scam. Third, the evidence of these scams is often contained in computer files, telephone records, and bank records that are subject to privacy laws and can only be obtained through a painstaking, laborious legal process. Moreover, even after being obtained, to decipher these records or acquire the computer information requires resources that may be unavailable to

local law enforcement and prosecutors. Finally, the cost in man-hours to identify evidence sources and draft the appropriate legal documents, and supplying out-of-pocket travel expenses for witnesses' and victims' court appearances makes the pursuit of these cases very cost-prohibitive. This is particularly true with the strong emphasis at the local level on investigating and prosecuting violent and narcotics crimes.

With all of the hurdles and problems that confront local law enforcement and prosecutors in combating telecommunications fraud, it is a wonder that any of these cases are prosecuted—but they are. In fact, in a survey of 310 local prosecutors' offices conducted by APRI in 2003, nearly 70 percent of the responding offices stated that their office had prosecuted a telecommunications fraud case within the past year.[1] Local prosecutors are pursuing these cases because frequently they are the only prosecutorial authority in a position to achieve justice on behalf of telecommunications fraud victims. United States attorneys' offices generally have dollar thresholds for indictment of financial crimes, and state attorney general offices sometimes lack criminal authority or have their own dollar thresholds.

Based upon the responses to the 2003 survey, APRI selected three prosecutorial offices for an in-depth study on what local prosecutors were doing to meet the challenges posed by telecommunications fraud cases. The offices selected were in three different regions of the country, with widely varying demographics: the San Diego County (CA) District Attorney's Office's CATCH Response Team[2]; the District Attorney's Office for the Thirteenth Prosecutorial District of North Carolina; and the Lake County (IL) State's Attorney's Office. Each of these offices has addressed the scourge of telecommunications fraud within the constraints of its manpower, investigative resources, and budget. APRI visited these offices with the goal of identifying the lessons learned and promising practices developed by these offices. The remainder of this monograph will provide an overview of each jurisdiction's demographics and discuss their respective efforts.

[1] This survey is documented in the APRI Special Report (September 2004), *If It Sounds Too Good To Be True: Local Prosecutors' Experiences Fighting Telecommunications Fraud*.

[2] CATCH is an acronym for Computer And Technology Crime High Tech Response Team.

JURISDICTION PROFILES

The three jurisdictions visited differ greatly in population, geographic location, and demographic characteristics. In addition, the law enforcement profile for each jurisdiction is reflective of these characteristics. The office having the largest population and area is San Diego County, a major metropolitan area that includes both the city of San Diego and its surrounding suburbs. The San Diego County District Attorney's Office's CATCH Response Team reflects the large population and excellent resource base with a structured and extensive unit comprised of personnel from local, state and federal law enforcement agencies. Because CATCH is a multi-county task force, it covers urban, suburban, and rural areas. The Lake County State's Attorney's Office (Lake County SAO) contains the second highest population and is largely a suburban jurisdiction with a retail-driven economy. Lake County has more than 40 incorporated municipalities, many with their own police departments. While the Lake County SAO has joined and formed task forces to combat telecommunications fraud, the primary emphasis has been on conducting investigations out of the office or assisting police agencies on an *ad hoc* basis. The least populated jurisdiction visited, the Thirteenth Prosecutorial District in North Carolina, is largely rural with a smattering of vacation and retirement communities. The visit to the Thirteenth Prosecutorial District concentrated on the most populated county within the jurisdiction, Brunswick County. Similarly to Lake County, the Thirteenth Prosecutorial District contains a number of municipalities, each with their own police department. However, the Thirteenth Prosecutorial District does not operate or participate in any telecommunications fraud task forces and works with the investigating agency on an as-requested basis. A more detailed description of the jurisdiction demographics and law enforcement profile for each jurisdiction follows.

San Diego County (CA) District Attorney's Office's CATCH Response Team

Three jurisdictions participate in CATCH: San Diego, Riverside, and Imperial Counties. These three counties vary widely in population, geog-

raphy, and industry. San Diego County is the most populous jurisdiction with more than 2.9 million people, followed by Riverside County with nearly 1.7 million people, and Imperial County with approximately 127,000 people. CATCH's jurisdiction encompasses the City of San Diego, suburban locales, such as Mission Hills, and rural areas. San Diego County has a significant high tech industry and is home to Nokia, Ericsson, Motorola, and Qualcomm. Riverside County was the fastest growing county in California during the 1990s and has a diverse economy with some high tech industry. Imperial County is largely rural, with an agriculture-based economy.

CATCH began operations in June 2000, and is one of five regional high tech crime task forces in California. The impetus for CATCH's formation was that prior to its inception, local law enforcement agencies were handling high tech crimes on an *ad hoc* basis and running into jurisdictional issues. CATCH is funded by a state grant with matching funds from the San Diego District Attorney's Office. Since its inception, CATCH's funding has grown from approximately $400,000 to more than $3 million. Likewise, CATCH staffing has increased from one prosecutor and four investigators to five prosecutors and 40 investigators. Nearly 20 federal, state and local agencies participate in CATCH, detailing personnel on a full or part-time basis, including the following:

- California Department of Justice (P)[3]
- California Department of Motor Vehicles
- Carlsbad Police Department
- Defense Criminal Investigative Agency
- Drug Enforcement Agency
- Federal Bureau of Investigation
- Immigrations and Customs Enforcement
- Imperial County District Attorney's Office
- Internal Revenue Service
- Office of the Inspector General
- Riverside County Sheriff's Department
- Riverside County District Attorney's Office (P)
- Riverside County Probation Office

[3] Agencies providing a prosecutor(s) and an investigator(s) are denoted with a (P).

- San Diego County Sheriff's Department
- San Diego Police Department
- San Diego County District Attorney's Office (P)
- San Diego County Probation Office
- United States Postal Inspection Service
- United States Secret Service

Lake County (IL) State's Attorney's Office

Lake County is a suburban jurisdiction located 40 miles from downtown Chicago in the northeast corner of Illinois. The population of Lake County is more than 685,000, with a significant Hispanic and Russian representation. The median household income for Lake County is the highest in Illinois at more than $66,000 per year, which exceeds the median household income for Illinois by more than $20,000. The population also is very well educated with nearly 40 percent of persons over 25 having a college degree or higher. However, Lake County contains significant disparities within its jurisdiction with wealthy communities such as Lake Forest (median household income of $136,462) and moderate-income areas such as the county seat, Waukegan (median household income of $42,335). The vast majority of employment in Lake County is in the retail or service industry.

Lake County has more than 40 local police agencies with only one, the Lake County Sheriff's Office having countywide jurisdiction. The local police departments primarily handle criminal investigations. The Lake County SAO is a member of the Chicago Metropolitan Identity Fraud Task Force (CMIFTF), and provides and receives assistance from that task force on an *ad hoc* basis. The Lake County SAO has a Computer Crimes Unit, which is comprised of an assistant state's attorney and a computer forensic analyst. Another investigator is informally detailed to the unit and works on investigations as his time permits. Otherwise, investigation is done by the local police agency with jurisdiction over the crime. In addition, the Lake County SAO has formed the Lake County Cyber Crime Task Force (Lake County CCTF).

District Attorney's Office for the Thirteenth Prosecutorial District of North Carolina

The Thirteenth Prosecutorial District of North Carolina is comprised of Brunswick, Columbus, and Bladen Counties with populations of 79,000, 55,000, and 33,000, respectively. All three counties are largely rural with small towns and communities. Brunswick County is on the coast, while Bladen and Columbus Counties are inland. Like many coastal communities, Brunswick County is a hotbed for vacationers and retirees, and it has the oldest median population in North Carolina. Brunswick County also borders with South Carolina.

The primary office for the Thirteenth Prosecutorial District is located in Brunswick County (Brunswick County District Attorney's Office (DAO)). More than half of the Brunswick County DAOs estimated 3,000 annual felony offenses occur in Brunswick County, and most of their fraud cases also arise there. At this writing, the Brunswick County DAO has 404 cases involving some type of fraud (not all of which are telecommunications fraud). The district attorney has designated one assistant district attorney to prosecute fraud cases, including telecommunications fraud. Because the vast majority of telecommunications fraud cases in the Thirteenth Prosecutorial District come from Brunswick County, the site visit gathered information about this county.

Brunswick County has 14 local police agencies with only one, the Brunswick County Sheriff's Office (BCSO), having countywide jurisdiction. The local police departments primarily handle criminal investigations. Coordination between local police agencies occurs on an *ad hoc* basis and is largely driven by individuals from the different agencies working together on their own initiative. No formal protocol or mechanism exists to ensure the exchange of information. There also is no mechanism for cooperation with law enforcement agencies across the state border. The primary goal of local law enforcement in fraud cases is to obtain restitution for the victim, which is critical because often the victim is a small business that is greatly impacted by the cost of the fraud. Typically, the investigating agency contacts the Brunswick County DAO when the suspect has been identified. At that time, the Brunswick County DAO will make a charging decision or request further investigation.

CURRENT TELECOMMUNICATIONS FRAUD SCHEMES

CATCH, the Lake County SAO, and the Brunswick County DAO experienced similar types of telecommunications fraud crimes. Scams experienced by all three jurisdictions included online auction fraud, credit card fraud, and identity theft. The biggest hurdle in investigating these types of crimes for law enforcement was identifying the perpetrator, particularly in re-mailing and identity theft scams involving stolen credit card numbers. The Lake County SAO noted that the critical step is determining the point of compromise of the stolen credit card number or personal information. Identification of the point of compromise narrows the pool of potential suspects and may reveal other incidents associated with the investigated scam. In addition, CATCH and the Lake County SAO reported that computer and network intrusions were a major problem within their jurisdictions. None of the offices reported that traditional telemarketing fraud was a major crime issue.

Internet Fraud

CATCH reports that the vast majority of the Internet fraud cases involve online auction schemes in which the seller does not deliver the item(s) or delivers an item of vastly inferior quality to the buyer. CATCH also has investigated Internet sales of bootleg items such as unauthorized satellite TV receiver access cards or pirated software. Because of limited resources, CATCH has an informal threshold of $10,000 or ten victims before they take investigative responsibility. Generally, the Internet fraud cases have involved perpetrators located within CATCH's jurisdiction. However, on occasion CATCH has investigated perpetrators in other jurisdictions when the case was proactively initiated and in coordination with a law enforcement agency with jurisdiction over the perpetrator's location.

Online auction fraud is probably the next most predominant fraud in Lake County, where the typical scenario involves sellers who do not send the purchased items on multiple occasions. Similarly, one of the biggest telecommunications fraud cases in Brunswick County involved a furniture company that advertised on the Internet but did not deliver the merchandise ordered. This case involved over 450 victims and more than

$2.5 million in aggregate losses. The victims were located throughout the United States, and the suspect reopened this operation across the state border in South Carolina, after being the subject of a search by the Brunswick County Sheriff's Office. Complaints of Internet auction fraud have not been pursued because of a lack of jurisdiction over where the money was spent.

Remailing

"Everything involves e-mail now," stated Lake County Assistant State's Attorney (ASA) Patricia Fix, in discussing current telecommunications fraud scams. The most predominant current online fraud scam in Lake County is "remailing," where perpetrators have go-betweens order high-end electronics on the Internet using stolen or fraudulent credit card numbers. The go-betweens then take delivery of the merchandise from the retailer and then remail it overseas. Another type of scam involves online solicitation, where the victim will respond to a spam e-mail, provide payment through a credit card, money order, or cashier's check, and not receive the merchandise or services purchased.

Credit Card Fraud

Credit card fraud is the most prevalent fraud crime being perpetrated in Brunswick County. As a summer vacation destination, Brunswick County has a transient population that peaks during the summer months. During the summer, fraud increases because more people are in the area and more businesses are open. Local businesses, many of which are seasonal and family-owned, are the most susceptible to fraud. Temporary employees steal customers' credit card numbers and use them to purchase merchandise over the Internet, or customers use stolen credit cards to obtain merchandise from the local businesses. Another common credit card scam is credit card reversal, where the perpetrator will use a customer's credit card number to reverse the payment to the merchant to the perpetrator's credit card.

Identity Theft

While some identity thieves have begun to use the Internet and computers to facilitate their crimes, the CATCH identity theft investigators noted that most identity theft was still committed through mail theft, vehicle and residential burglaries, dumpster diving, and forgery, particularly check washing.[4] A growing tactic involves perpetrators obtaining office jobs with access to personal information which they steal. Some of the high tech identity theft schemes CATCH investigators have encountered include phishing, spoofing, and spam scams.[5] CATCH investigators also have noted a relationship between identity theft and narcotics use (particularly methamphetamine) and gambling. Similarly, Brunswick County has noted identity thieves using counterfeit and forged checks.

Computer and Network Intrusion

CATCH and the Lake County SAO both have cases involving unauthorized access to computer networks and databases, also known as "hacking." The motive behind many of these hacking incidents is to obtain personal identifying information or make use of the network resources to store data or send e-mail. In contrast to Internet fraud cases, nearly all the computer and network intrusion cases investigated by CATCH involve San Diego or Riverside victims with perpetrators located outside California. For example, one high-profile network intrusion case involved a hack into the University of California-Riverside's computer network by perpetrators located in Great Britain. The biggest source of frustration reported by CATCH and the Lake County SAO regarding these types of cases is the private sector's reluctance to report network intrusions.

[4] "Check washing" describes the process whereby identity thieves take checks and use a chemical to erase the name of the payee and they then substitute another name. The identity thief will then cash the check under that name.

[5] "Phishing" occurs when the perpetrator establishes a fraudulent Web site and entices victims to provide identity, credit card, and/or banking information; spoofing occurs when the perpetrator disguises his or her actual e-mail address when sending an e-mail to entice a response from the victim; spamming is sending unsolicited e-mails en masse to market a product or service.

ENFORCEMENT

Enforcement issues in telecommunications fraud cases have centered around two issues: (1) organizing the investigation effort; and (2) utilizing efficient investigative tactics in terms of man-hours and production of relevant evidence. Each jurisdiction's enforcement effort is reflective of the resources available. CATCH's use of a task force approach has been enhanced by the infusion of state funding. The Lake County SAO also has used a task force approach but as more of a supplemental resource than as a joint investigative agency. The Lake County SAO also has focused more on investigating cases "in-house" and providing assistance on a case-by-case basis. The Brunswick County DAO has focused a great deal of effort on victim assistance to ensure victims are informed of case status and receive restitution. Particularly for the Brunswick County DAO, a lack of access to digital evidence analysis resources has hampered enforcement efforts.

The Task Force Approach

CATCH and the Lake County SAO have used the task force approach to address the multi-jurisdictional and labor-intensive nature of telecommunications fraud investigations. CATCH is a joint investigative task force operating under the supervision of the San Diego County District Attorney's Office. The Lake County SAO participates in the Chicago Metropolitan Identity Fraud Task Force (CMIFTF) and also has its own Cyber Crime Task Force. While the Lake County SAO does not conduct joint investigations in the manner of CATCH, these task forces have proved excellent vehicles for exchanging intelligence and obtaining additional manpower when needed. The Brunswick County DAO does not have a task force and there is no task force within the area. However, the North Carolina State Bureau of Investigation (NCSBI) and the FBI have launched a task force, entitled Fast Cops, which will have federal, state and local law enforcement involvement.

The experience of CATCH, the Lake County SAO, and the plans for Fast Cops are discussed in greater detail below. However, in establishing a

task force six issues were of paramount concern in all of these efforts:

- Establishment of a clearly defined mission and goals for the task force. Is the task force an information exchange and investigation coordination mechanism or a joint investigative task force?
- Identification of potential members whose involvement is consistent with the task force mission and goals. Will private organizations be included?
- Identification of the agency to lead the task force and clearly defining the role of each member.
- Requirement for some sort of resource commitment from the members.
- Exploration of the possibility of outside funding for the task force from federal, state, or local grants or private contributions.
- Periodic reexamination of the task force mission, goals, membership, and resource contributions to ensure that the task force remains relevant and does not become just another monthly meeting.

CATCH

As previously noted, CATCH is comprised of 19 federal, state, and local law enforcement agencies. Each agency has entered into a formal Memorandum of Understanding (MOU) with the San Diego County District Attorney's Office to define the scope of each agency's commitment to CATCH. Especially important is the agencies' commitment to assign personnel for an extended time period (generally three years) because of the extensive training required to investigate high tech crimes.[6]

CATCH has a formalized mission statement and protocols for accepting, investigating, and prosecuting cases. For cases involving online fraud, CATCH generally requires that the losses attributable to a scam exceed $10,000, or that there are ten or more victims. The rule of thumb is to investigate cases that appear to have the most severe criminal liability for the perpetrator in comparison with the amount of time needed to investigate. CATCH initiates investigations in two primary ways: referrals from other law enforcement agencies, particularly the U.S. Secret Service Fraud Task Force; and consumer complaints referred from the Internet

[6] CATCH has noted reluctance on the part of smaller law enforcement agencies to detail personnel. To address this concern, CATCH plans to set up two open workstations and invite non-participating agencies to send personnel to conduct investigations from these stations.

Fraud Complaint Center.[7]

CATCH high tech crime investigators are divided into four teams, each with its own team leader. All prosecutors are available to consult with the teams and there is an on-call prosecutor at all times. The CATCH project director, who is a San Diego County deputy district attorney, assigns cases to prosecutors.[8] Normally, once a prosecutor becomes involved in working with a team on an investigation, that prosecutor will continue to work that case until final disposition.

The primary CATCH office is located in San Diego County and houses three teams and four of the prosecutors. CATCH has a satellite office in Riverside County, which houses the other team and a deputy district attorney from the Riverside County District Attorney's Office. CATCH has an on-call investigator available to take citizens' complaints and provide technical assistance to law enforcement agencies. Generally, the citizen complainants are referred to the appropriate local law enforcement agency unless the complaint appears to meet CATCH criteria or is of an exigent nature.

In May 2002, CATCH expanded to form an identity theft team in response to a growing number of identity theft complaints. The identity theft team is housed at the main CATCH office and primarily obtains its cases through a unique, proactive approach of conducting searches of probationers' residences pursuant to Fourth Amendment rights waivers executed by probationers at the time of their guilty pleas. The identity theft team also accepts a limited number of referrals from other law enforcement agencies.

CATCH is a state-of-the-art high tech crime investigation unit, which has successfully integrated local, state, and federal law enforcement agencies, prosecutors, and investigators to achieve a common goal of combating high tech crime. CATCH's success is demonstrated through its

7 IFCC is a consumer complaint center and database operated by the Federal Bureau of Investigation and the National White Collar Crime Center.

8 If the case has a federal nexus and meets the filing guidelines for the U.S. Attorney's Office for the Southern District of California, the investigator also may choose to present the case for federal prosecution. Generally, a federal agent will then work with the state investigator on the case.

tremendous growth, with the personnel and budget both quintupling in a four-year span in response to an exploding caseload.[9] CATCH personnel cited four factors critical to its success:
- Clearly defining the goals of CATCH;
- Balancing available resources with prospective workload;
- Identifying participating agencies consistent with CATCH's goals; and
- Obtaining long-term commitments from the participating agencies.

CATCH's definition of its goals and development of a protocol for case acceptance helped ensure that CATCH balances manpower and workload. It also ensures that CATCH is not duplicating the effort of other task forces, such as the San Diego Internet Crimes Against Children Task Force. Having federal, state, and local agencies participate provides CATCH with greater resources to cross jurisdictional boundaries, as often occurs in investigating telecommunications fraud crimes.[10] Also, with a wide array of agencies participating, when an agency has to reduce its commitment temporarily, as the FBI did in the wake of September 11, 2001, and the U.S. Secret Service did in the past presidential election year, the effect is not so drastic. Formalizing the commitment through MOUs has helped make certain that those agencies returned to CATCH and has also reduced personnel turnover. This is important because the training required to both investigate and analyze digital evidence is extensive and it is impossible to constantly train new personnel.

Lake County Cyber Crime Task Force

In 2003, the Lake County SAO formed the Lake County CCTF to coordinate investigations involving crime committed using computers. The task force members are the Lake County SAO, the Lake County Sheriff's Office, and the Vernon Hills Police Department. There are no formal task force meetings nor is there a formal organizational structure. The Lake County CCTF does maintain a point-of-contact list and educational materials to use for consumer education trainings on Internet safety and protecting yourself from identity theft. These materials are

9 From July 2001 to August 2003, CATCH had investigated 611 defendants, assisted other agencies in 106 investigations, conducted 131 forensic examinations, arrested and charged 217 defendants, and convicted 168 defendants.

10 Having agencies from different levels of government can become particularly important when officers cannot be cross-sworn because of liability or other issues.

available on the law enforcement access only part of the Lake County CCTF's Web site, www.co.lake.il.us/statesattorney/cctf/. The Lake County SAO's establishment of its own computer crime task force, the CCTF, demonstrates the importance of coordination at the local level between agencies of smaller jurisdictions and agencies with countywide jurisdiction. Currently, the Lake County SAO's dearth of manpower prevents it from taking a more active leadership role in the CCTF. If the Computer Crime Unit for the Lake County SAO is able to obtain more personnel, expanding the Lake County CCTF's role and using it to coordinate joint investigations may be feasible.

Chicago Metropolitan Identity Fraud Task Force

The Lake County CCTF serves as the SAO's representative to the CMIFTF. The FBI formed the CMIFTF in March 2003 to address the growing problem of fraud-related identity theft, especially the use of fraudulent or stolen credit card numbers to purchase merchandise using the Internet.[11] The CMIFTF is a mix of federal, state, and local law enforcement agencies, local prosecutors' offices, and private sector companies. The following organizations are members of the CMIFTF:

- Federal Bureau of Investigation
- United States Postal Inspection Service (USPIS)
- Illinois Attorney General's Office
- Illinois State Police
- Lake County State's Attorney's Office
- DuPage County State's Attorney's Office
- Will County State's Attorney's Office
- Chicago Police Department
- Oak Park Police Department
- Vernon Hills Police Department
- Matteson Police Department
- Cook County Adult Probation
- Marshall Fields
- Target
- Circuit City
- Discover Card
- Harris Bank

[11] Additional background information on the CMIFTF may be found at its Web site at www.cmiftf.org.

The CMIFTF meets bi-monthly at space provided by Marshall Fields, which also provides office space to house the task force nucleus—an FBI special agent, who is the task force leader, a Chicago Police Department detective, and a USPIS inspector. All CMIFTF member agencies have entered into a Memorandum of Understanding (MOU), which requires that each participating agency assign an officer. Assigned local police officers are cross-deputized as U.S. Marshals so that they can perform police functions outside their home jurisdictions. The purpose of the task force is for the members "to combine their investigative services, employees, and other resources for the purpose of enforcing laws prohibiting the theft of identity and the fraudulent use of financial transaction devices[.]"[12]

The CMIFTF essentially operates in three ways. First, the nucleus of the task force conducts identity theft investigations out of the office space provided by Marshall Fields. Second, task force members call upon each other for manpower when needed to execute large-scale arrests or search warrants. Third, the task force serves as an information clearinghouse regarding current cases and scams between law enforcement agencies and corporate fraud units.

In July 2004, the CMIFTF leadership solicited from participating agencies suggestions to improve the efficiency and utility of the task force. Suggestions from the member agencies included:

- Rotating the location for the bi-monthly meeting to increase participation;
- Increasing communication among members through e-mail, particularly to provide timely alerts of current scams and obtain additional manpower if needed;
- Recruiting and funding of confidential informants;
- Full-time staffing;
- Participation by Immigration and Customs Enforcement;
- Improving call-out system for law enforcement officers, particularly for controlled deliveries of fraudulently obtained merchandise;
- Participation by UPS and Federal Express, since they frequently ship fraudulently obtained merchandise;

[12] As stated in the MOU between the Lake County SAO and the FBI.

- Participation by EBAY and PayPal, since many complaints involve them;
- Holding an annual or semi-annual conference;
- Making the task force a non-profit organization to facilitate private sector contributions; and
- Increasing prosecutor participation at the local and federal level to ensure that "fileable" cases are being investigated.

The CMIFTF is an important first step in a regional approach to attacking identity theft. Unfortunately, the CMIFTF has not been successful in convincing local law enforcement that task force participation is beneficial, as several local law enforcement officers commented that the task force only requested assistance and did not provide it. The Lake County SAO's participation in the CMIFTF has alleviated some of its manpower limitations especially when needing extra manpower to execute a search warrant. Unfortunately, the CMIFTF has not resulted in facilitating joint investigations, which could be particularly helpful, particularly in the remailing scams where the merchandise is ordered in one jurisdiction and delivered in another. An encouraging note is that CMIFTF leadership recognizes the task force's current limitations and is taking steps to address them.

FAST COPS Task Force

The Brunswick County DAO does not have any fraud task forces to participate in within its area. However, there is an effort to establish a fraud task force in central North Carolina known as Fast Cops. To quicken the pace of fraud investigations and fill communication gaps caused by jurisdictional limitations, the FBI, the U.S. Attorney's Office for the Eastern District of North Carolina, and NCSBI were starting the Fast Cops task force in summer 2004. The task force is based on a tier system with the FBI, U.S. Attorney's Office, and NCSBI on the first tier and the U.S. Secret Service, local police agencies, and civil authorities on the second tier. The task force will meet monthly with the initial focus on Wake County in central North Carolina. To encourage participation at least initially there will be no requirement to contribute manpower. After establishing the task force in Wake County, the plan is to expand the task force to include other jurisdictions within North Carolina. The benefit to state and local authorities will be the ability to call upon the manpow-

er and expertise of federal agencies in investigating these cases. Federal agencies will benefit because quite often it can be faster to obtain state search and arrest warrants.

Public-Private Cooperation

CATCH and CMIFTF both have made use of private resources to enhance their effectiveness. CATCH consults with a steering committee that is comprised of 30 companies and educational institutions. The steering committee meets quarterly and provides CATCH the opportunity to educate the private sector about current scams. The steering committee also provides a forum for CATCH to work with the business community to develop protocols for obtaining investigative information and alerting the community of threats and scams. CMIFTF has gone even further by including corporate members in the task force. These corporate partners have provided important resources such as office space, administrative support, and investigative assistance.

Another benefit to public-private cooperation is that in telecommunications fraud, unlike other crimes, much of the physical evidence is located in records possessed and maintained by the business community. Potentially relevant records include bank account transactions, money transfers, shipping records, telephone records, and Internet Service Provider (ISP) subscriber, transactional, and content information. Knowing what information is in the possession of the corporations and financial institutions, whom to contact to obtain that information, and how long the records are maintained can be critical to the success of an investigation. Including the business community in the task force can establish informal lines of communication that can ensure records are preserved and minimize the amount of searching for the correct records custodian. Decreasing the effort and time needed to obtain records was a major impetus in CMIFTF's effort to add Federal Express and UPS to the task force.

Funding

Agencies desiring to start a telecommunications fraud task force should be alert to possible funding opportunities at the federal, state, and local levels. At the federal level, agencies may want to monitor funding opportunities offered by the U.S. Department of Justice's Office of Justice Programs. Opportunities to attend training in collecting and analyzing digital evidence also may be available through the FBI, the Federal Law Enforcement Training Center or the Regional Computer Forensics Laboratory in an agency's area. At the state level, frequently a computer crime unit or task force exists that may have information about funding sources. In planning a task force, agencies also may want to consider in-kind participation such as detailing personnel, equipment loans, or furnishing of office space.

All three sites demonstrated an awareness of state funding opportunities. CATCH started with a state grant and subsequently expanded to target identity theft through another state grant. In response to the increase in telecommunications fraud cases, the Lake County SAO has applied for a state grant to increase their resources. If received, the Lake County SAO will use the grant to hire a victim's assistance coordinator for community outreach, helping repair damages caused by identity thieves and keeping victims informed of case status and disposition. The Brunswick County DAO also applied for a grant sponsored by the North Carolina Governor's Commission on Crime Control. If awarded the grant, Brunswick County will receive an additional prosecutor, investigator, and administrative person to deal specifically with identity theft and financial fraud cases. The additional manpower would allow the Brunswick County DAO to facilitate increased cooperation at the local level among the 14 local police agencies in investigating telecommunications fraud.

CATCH found that reliance on asset forfeiture to fund a task force was not feasible because seized computer equipment frequently had marginal value. In contrast, the Lake County SAO was able to use forfeited equipment and proceeds to establish its own computer lab. While such forfeitures may not be reliable funding streams, they can provide "one-

time" boosts for equipment purchase and provide seed money to start new programs as demonstrated by the Lake County SAO.

Investigative Tactics

In terms of investigative tactics, most investigations of telecommunications fraud cases in the visited jurisdictions proceed in a traditional manner, i.e., a complaint is received, law enforcement investigates the complaint by interviewing witnesses and using legal process to collect the physical evidence, and the collected evidence is analyzed. However, the successful tactics used by each jurisdiction have some commonality:

- involve prosecutors in the case as soon as possible and conduct vertical prosecution to ensure the appropriate legal process is used, the number of investigations for declined cases are reduced, and establish a rapport with the victim;
- obtain digital evidence using the appropriate legal process as soon as possible because the data is fragile and may be deleted;
- have digital evidence analysis and recovery resource back-ups, backlogs are growing because more digital evidence is being seized, requiring more time to analyze;
- digital evidence analysis is considered a supplement to, but not in lieu of, traditional police investigative tactics, particularly witness and suspect interviews; and
- provide victim assistance, because frequently victims suffer grievous financial impact and are bewildered by the complexities of obtaining restitution or repairing damage to their credit history.

Prosecutor-Investigator Cooperation

Housing prosecutors and investigators together was cited by CATCH personnel as critical to success. Telecommunications fraud investigations nearly always require issuance of search warrants, and prosecutorial review can ensure that the warrants comply with applicable constitutional and statutory requirements. Having prosecutors in-house makes certain that these warrants are reviewed as soon as possible so that digital evidence is obtained in a timely manner. Obtaining digital evidence quickly is important because there are no statutorily required periods for ISPs to retain digital evidence and important evidence can be erased or overwritten. In

addition, this enables investigators and prosecutors to discuss what evidence is necessary to charge the case. This can be particularly important in fraud cases, where fraudulent intent often needs to be proven through circumstantial evidence. CATCH utilizes vertical prosecution, i.e., one prosecutor and lead investigator stay with the case from initial assignment to final disposition. Vertical prosecution limits the duplication of effort needed to brief a newly assigned prosecutor or investigator. The Lake County SAO also practices vertical prosecution on complex telecommunications fraud cases and the prosecutor, investigator and forensic analyst work closely together on all investigations.

Search Warrants

For CATCH, the primary investigative tool is a search warrant because California law generally does not provide law enforcement with pre-charging subpoena power. CATCH investigators identify the lack of pre-filing subpoena power as one of the biggest challenges because drafting search warrants, the underlying probable cause affidavits, and warrant returns is very time consuming. A typical case requires issuance of three to five search warrants. CATCH investigators noted the importance of coordinating warrant responses with ISPs and with the right person within the ISP to ensure that the ISP produces the information or records sought. Because CATCH policy is that a prosecutor must review all warrants prior to submission to a judge, it is critical that a prosecutor be available. CATCH investigators unanimously stressed the importance of housing the prosecutors with investigators for rapid response and ensuring communication in these complex cases.

Because Illinois and North Carolina both have grand jury subpoena power, search warrants are not used as commonly as in California to obtain evidence. Generally, a search warrant is used only to search the suspect's location(s) and obtain e-mail content information from ISPs. Normally, the Lake County SAO drafts a search warrant for digital evidence, which incorporates the officer's statement of probable cause. For the Brunswick County DAO, prosecutorial review occurs only when contacted by the law enforcement agency seeking the warrant or if the prosecutor previously has been involved in the case.

Grand Jury Subpoena

The Lake County SAO has found the issuance of grand jury subpoenas to be the most economical and effective method of collecting evidence. Grand jury subpoena power enables the investigating agencies to gather most of the evidence with only a minimal amount of paperwork time. Grand jury subpoenas typically are used to gather information from neutral sources, particularly financial institutions. The process to obtain these subpoenas is very streamlined, with officers able to obtain them by telephone from the Lake County SAO. On average, the Lake County SAO has found that the investigation of a telecommunications fraud case requires the issuance of six to ten grand jury subpoenas and one search warrant.

Probation Waivers & Searches

CATCH initiated its identity theft team in May 2002, using state funding. The challenge for CATCH was to develop a program that could have an impact with limited funding and manpower. CATCH decided to focus its efforts on a proactive approach of identifying identity theft perpetrated by probationers and parolees. The primary investigative tactic used in this effort is probation searches conducted pursuant to probationers' Fourth Amendment rights waivers. Search targets are identified from tips by confidential informants, probation officers, or from the probation office's database. This approach has been very successful in generating identity theft cases because many identity thieves are recidivists. Investigators for CATCH emphasized the importance of the participation of the San Diego County Probation Office and United States Postal Inspection Service (USPIS) on the identity theft team. The USPIS's participation is important because much of the stolen personal information is gathered through mail theft and because identity thieves frequently use stolen identities to order merchandise that require mail delivery.[13]

Wiretapping

The interception of communications on a real-time basis, also known as wiretapping, is not a tactic frequently used by CATCH because it is too resource intensive, both in equipment costs and in personnel to monitor

[13] The importance of working with the USPIS on telecommunications fraud investigations was echoed by both the Lake County SAO and the Brunswick County DAO.

the communications lines. The Lake County SAO makes greater use of wiretapping simply because Illinois, as a two-party consent state, requires a judicial order to record any telephone or on line communications on a real-time basis. However, because of stringent statutory requirements, the Lake County SAO noted that wiretap orders are time consuming to prepare.

Suspect Interview

Brunswick County law enforcement agencies report that suspect interviewing is the best tool available in investigating telecommunications fraud cases. Most fraud suspects are very willing to discuss their crimes and even brag about their exploits. Through the interview, investigators can persuade suspects to grant consent to a search of their home, computer, or any area necessary to discover evidence of a crime. Brunswick County's success with suspect interviews is an important reminder that while telecommunications fraud may involve collecting and analyzing high tech evidence, this is in addition to—not in lieu of—traditional police investigation methods.

Evidence Storage

CATCH maintains its own evidence storage facility and is implementing a bar code inventory system to track evidence. This makes it easier for CATCH to process the evidence without having to go off-site. With so many different agencies participating in CATCH, maintenance of evidence at each agency's "home" evidence facility would be a logistical nightmare. By maintaining its own evidence facility, CATCH streamlines the chain-of-custody and ensures evidence can be located promptly when needed for trial.

Investigative Resources

Databases, list serves, and contact lists are important for identifying perpetrators, linking incidents arising from a common scam, and overcoming jurisdictional barriers to obtaining evidence and locating suspects. CATCH, the Lake County SAO, and the Brunswick County DAO all have found databases and contact lists to be of great assistance in investigations. An investigative asset noted by CATCH investigators was access to the Regional Justice Information System, a regional database with infor-

mation input by local government and law enforcement agencies throughout San Diego County. The Lake County SAO uses several databases and list serves in investigating telecommunications fraud. These databases include the Illinois Secretary of State's databases of corporate filings and driver's license photos, the Illinois Department of Corrections' inmate information database, the Lake County property records database, and the commercial database, Autotrack. However, there is no regional database for reporting scams, which would be very useful in trying to identify complaints with a similar factual basis to see if they are related. The Brunswick County DAO has a countywide database that contains arrest and booking information. Access to the database is available to law enforcement for a monthly fee. Expanding the information and use of this database may help investigators identify perpetrators who are running scams in multiple police jurisdictions within Brunswick County.

Regarding list serves, the Digital-DA list serve was noted as particularly useful to discuss digital evidence search and charging issues.[14] CATCH and the Lake County SAO also cited training rosters from classes attended with law enforcement officers from other states and the membership list-serve for the High Technology Crime Investigation Association as especially useful.[15]

Digital Evidence Analysis Resources

Many telecommunications fraud schemes use computers to facilitate the scams. Whether through spam e-mail, phishing, or maintaining call lists, scripts, and records by a traditional telemarketing fraudster, digital evidence is a part of nearly every telecommunications fraud investigation. However, acquiring the digital evidence in a manner that maintains its integrity and sifting the relevant data from digital media requires specialized training. Therefore, it is imperative that when investigating telecommunications fraud cases, a law enforcement agency have or have access to digital evidence analysis resources. In addition, to ensure efficient and

[14] The Digital-DA list serve is run privately by Illinois Assistant Attorney General Abigail Abraham. To subscribe to the list serve, a person must be a state or local prosecutor who prosecutes cases involving digital evidence. State and local prosecutors interested in joining the list serve can obtain additional information by contacting whitecollar@ndaa-apri.org.

[15] More information regarding the High Technology Crime Investigation Association can be found at http://www.htcia.org/.

proper analysis of the seized digital media, it is very helpful if the investigator and examiner communicate to ensure the analysis of the digital media is for relevant evidence. This is especially necessary because the presence of digital evidence in all types of crimes is becoming more prevalent, the types of digital media are growing, and the analysis of that evidence is becoming more time consuming as the capacity of digital media to store data increases, creating backlogs for analysis.

CATCH has substantial in-house digital evidence analysis resources, with eight computer forensic analysts. If digital evidence needs to be analyzed as part of an investigation, the CATCH team leader will assign a computer forensic examiner and the investigator will complete a service request. The assigned examiner contacts the investigator after receipt of the request to discuss the conduct of the examination. Normally the examination is performed within 30 days of the service request. Most computer forensic examinations are done in-house with a limited number being referred to the San Diego Regional Computer Forensics Laboratory (RCFL).[16] CATCH has a written protocol for the collection and analysis of digital evidence. CATCH examiners identified two key criteria for digital forensic analysis: documentation of how and where the digital evidence is recovered from the examined media; and the ability to explain that process in layman's terms when testifying.

The Lake County SAO was able to fund the creation of a computer forensics lab through forfeiture of computer equipment and bank accounts in a telecommunications fraud scam. The Waukegan Police Department provided the computer forensics space and also has a computer forensics analyst that works closely with the Lake County SAO's analyst. In addition, several other local police departments in Lake County have in-house forensics capability. Police departments without in-house capability must submit their digital evidence for analysis to the Lake County SAO or the Illinois RCFL.

[16] The RCFL is a joint federal, state, and local computer laboratory run by the FBI. Information on the RCFL can be found at http://www.rcfl.org/. At the time of the site visit, CATCH investigators noted the RCFL had a six-month backlog in forensic examinations. In addition, the Riverside team does not have access to the RCFL and performs forensics for its own cases in-house; because of limited forensic capability, Riverside had a six- to seven-month backlog at the time of the site visit.

Only two police agencies in Brunswick County have limited in-house computer forensic capability, the Brunswick County Sheriff's Office and the Ocean Isle Police Department (OIPD). However, with both agencies, the computer forensic analyst is available only on a part-time basis as they also serve as investigators. The state-level police agency, the NCSBI, lacks sufficient computer forensic resources to examine computers seized in fraud cases because its resources are entirely devoted to child pornography and homicide cases.[17] However, the FBI and U.S. Secret Service have done computer forensics on behalf of the local agencies upon request. Brunswick County law enforcement noted that the lack of a full-time computer forensic analyst was a hindrance in telecommunications fraud cases. On the other hand, as the Brunswick County District Attorney pointed out, it is cost-prohibitive, particularly for smaller police agencies, to devote a person full-time to this area. What is needed is a resource that is available to all the local agencies. Unfortunately, the NCSBI has been unable to fill this role because it has prioritized other types of crime. Federal agencies have been responsive when the cases meet their guidelines. If the funding becomes available, the Brunswick County DAO may consider developing a countywide digital evidence analysis resource.

Victim Assistance

An important component of any telecommunications fraud investigation is victim assistance. Victim assistance can help establish a good rapport, which can aid in obtaining evidence from victims. Victims also frequently suffer a severe financial impact from these crimes, both directly through the financial loss itself and indirectly through damage to their credit ratings. Normally, a victim's only hope for restitution is through the criminal justice system and frequently a victim needs assistance in repairing the damage to his or her credit rating. Each of the visited jurisdictions provided some manner of victim assistance and emphasized restitution as a sentencing condition.

[17] The NCSBI lacks original jurisdiction over crimes and may only become involved in the investigation upon request from a local police agency.

CATCH seeks restitution in all cases where the defendant's crime causes financial injury to the victim(s). Generally, CATCH will initially contact the victim through e-mail and follow up with a telephone call to obtain restitution information. Court appearances are arranged through a witness coordinator. The Lake County SAO generally seeks restitution on all fraud cases; however, judges will order restitution only on charged incidents. Since many fraud cases often involve multiple incidents, obtaining full restitution for the victim can be problematic. Further, for sentencing purposes, losses can only be aggregated by victim, not by scam, which means that sentencing enhancements generally will not apply. Due to budget limitations, the Computer Crimes Unit for the Lake County SAO does not have a victim assistance coordinator. ASA Fix noted that one of the priorities for the unit, should it receive grant funding, is to hire a full-time victim assistance coordinator particularly to help victims of identity theft in the time-consuming task of clearing their credit history. Currently, because there is no victim assistance coordinator, victims are normally not contacted about the status or disposition of their cases. Victims are helped by a state law that provides that they only have to contact one of the three major credit service reporting agencies (CSRA) to clarify discrepancies; the contacted CSRA is then responsible for sharing this information with the other two CSRAs.

Seeking restitution on behalf of victims and keeping them informed as to case status is a priority with the Brunswick County DAO. The Brunswick County DAO seeks restitution in every case in which the victim has suffered some financial loss.[18] Upon indictment, the victim-witness legal assistant for the office sends a letter that notifies the victim of the indictment, future court dates, and requests that the victim provide an impact statement. The victim impact statement requests that victims describe the extent of personal injury, property loss, or other damages they may have incurred and current contact information. Upon final case disposition, the victim-witness legal assistant sends a letter to the victims informing them of any restitution ordered. Victim assistance workers also aid victims of credit card fraud or identity theft in notifying financial institutions and credit service reporting agencies to repair their credit

[18] Restitution is particularly important because fraud victims cannot receive compensation from the North Carolina Victims' Rights Fund, which is reserved for victims of violent crimes.

reports. In addition, for cases with older victims, the victim-witness legal assistant will sit with them during court proceedings. Staff members who engage in volunteer work in the community also inform the public of the services available to victims.

Law Enforcement Education

Law enforcement education is an integral part of all three visited jurisdictions' efforts to combat telecommunications fraud. Law enforcement education has focused on initial responders to ensure that they recognize telecommunications fraud as a crime and know what evidence to gather from a complainant and how to preserve digital evidence. Another aspect of law enforcement education has been to teach basic online investigative techniques, such as tracing e-mail or identifying Internet Protocol (IP) addresses,[19] so that the initial responder or investigator can perform more of the investigation, allowing specialized investigators time to concentrate on issues that are more complex.

CATCH has devoted a significant effort to educating the local law enforcement agencies within its jurisdiction. CATCH has two primary goals in this area: (1) making these agencies aware of CATCH's availability as a resource; and (2) educating first responders about preserving a crime scene containing digital evidence and basic evidence collection techniques, i.e., bag-and-tag training. Line-up training is generally used to make first responders aware of CATCH's availability as a resource. Bag and tag training is often conducted at the San Diego RCFL. CATCH's identity theft team also does fraudulent document recognition training for patrol and probation officers. This has the beneficial effect of ensuring that digital evidence collection is performed in a manner to protect the integrity of the evidence and lessens the need for CATCH to respond to calls for advice on basic evidence collection issues.

Initially, law enforcement training done by the Computer Crimes Unit for the Lake County SAO focused on detectives as the target audience for online investigative techniques. However, with the growth in complaints, the training focus has shifted to teaching first responders basic online investigative techniques such as tracing an IP address. The Lake County SAO also conducts basic bag-and-tag training for first responders on seizure of digital evidence at crime scenes. The office estimates that it

[19] IP addresses are the identifiers used by computers to route messages on a network, including the Internet.

has trained over 1,000 officers on bag-and-tag and basic online investigative techniques. The focus by the Lake County SAO on providing the first responders the basic knowledge to take the initial investigative steps helps to ensure that evidence is collected as soon as possible, which is particularly important given the fragile nature of digital evidence and the lack of industry standards for retention of digital evidence by ISPs. It also helps investigators by giving them a head start when they are assigned the investigation. This is particularly important because in cases involving digital evidence and fraud scams, perpetrators can easily delete digital evidence and often change their physical locations upon successful perpetration.

The Brunswick County DAO has been able to offer only limited training on telecommunications fraud. Further, even when training is available, due to the annual influx of tourists and seasonal residents, some local law enforcement agencies are unable to attend training sessions during the spring and summer months. This problem is further exacerbated by the fact that to stay current in this area requires continued training. The North Carolina Justice Academy provides basic bag-and-tag seminars for computer seizure. Computer forensic analysis training is available at the Piedmont Regional Criminal Justice Training Academy and the National White Collar Crime Center.[20]

[20] More information regarding the National White Collar Crime Center may be found at http://www.nw3c.org/.

PUBLIC EDUCATION

CATCH, the Lake County SAO, and the Brunswick County DAO all have developed public education materials to warn consumers about telecommunications fraud and identity theft and educate them on how to protect their information to avoid being victimized. Generally, these materials are distributed through live presentations to civic groups and neighborhood organizations. The goals of the materials are twofold: (1) alert consumers of the warning signs of telecommunications fraud scams to avoid being victimized; and (2) educate them about the steps they should take if they are victimized.

CATCH's public education efforts have been accomplished through public speaking and production of educational materials. Public speaking efforts have often involved presentations to senior citizen groups about online safety in computer usage and protecting one's identity. The educational material effort has centered on publication of a guide on wireless security. CATCH has noted a need for education on wireless security because of the increasing use of wireless networks at home and work. Unless these wireless networks are configured properly, they are open to unauthorized access and manipulation. CATCH's steering committee provides CATCH with an avenue of communication with the private sector and educational institutions, which may be the first to note trends in this area. The steering committee also provides CATCH with additional outlets to communicate its educational messages to the public.

Most of the Lake County SAO's prevention efforts focus on making presentations, which focus on protecting personal identification information, to civic and senior groups. The Lake County SAO makes available training materials for law enforcement to use to educate the public on the CCTF Web site. Unfortunately, due to manpower constraints, the Lake County SAO is unable to fulfill all the requests received for public presentations.

The Brunswick County DAO focuses on educating the community about types of fraud scams including telecommunications fraud. Trainings

are provided free of charge to local businesses, watch groups, and citizens. Currently, the Brunswick County DAO averages about three trainings annually, which are typically three days in length. The BCSO also educates the public on scams through its Crime Prevention program, which has conducted trainings for local civics groups and the AARP. The NCSBI also provides educational presentations with a heavy emphasis on alleviating false expectations by letting people know that many of their cases may not get investigated due to a lack of resources. Victims are told that they will, in all likelihood, have to do most of the legwork on their case.

Brunswick County Social Services issues scam alerts through senior centers and bulletins distributed as part of meals-on-wheels programs and churches. Ms. Evelyn Johnson, a social worker with Brunswick County Social Services, stated that public education regarding traditional telemarketing fraud has been very effective in increasing consumer awareness. FBI Special Agent Joan Fleming, who stated that AARP has been very effective in educating seniors about telemarketing fraud, particularly the "Don't Fall for a Phone Line" video, echoed this view. The Brunswick County Social Services method of distributing fraud alerts through senior centers and meals-on-wheels is useful in warning seniors about current scams. Unfortunately, no concomitant business roundtable or organization exists to provide fraud alerts to local businesses. In addition, there is no system or mechanism for law enforcement and the business community to exchange information about ongoing scams.

Conclusion

Telecommunications fraud presents unique difficulties for investigation and prosecution. Foremost is the multi-jurisdictional nature of the crime, which requires local prosecutors and law enforcement to cross jurisdictional boundaries to collect evidence and locate perpetrators or victims. Next is the labor-intensive nature of telecommunications fraud investigations, which arises from several factors including:

- telecommunications fraud schemes typically involve multiple incidents of fraud;
- these multiple incidents often occur in widely separated places;
- identifying the perpetrator of a scheme can require collecting evidence from numerous sources such as financial institutions, shipping companies, ISPs, and telephone companies; and
- obtaining records from these companies can be difficult, requiring very specific legal process.

Finally, because telecommunications fraud nearly always involves digital evidence and financial records, expertise in financial investigations and access to digital evidence resources greatly improve the odds of a successful investigation leading to the apprehension of the perpetrator(s).

Three different jurisdictions with greatly varying demographics have attacked the problem of telecommunications fraud in manners consonant with the resources and priorities of their respective areas. CATCH has overcome these difficulties by building a "one-stop shop." CATCH is a fully integrated task force with participating federal, state, and local agencies, with in-house prosecutors and digital evidence analysis resources. By concentrating prosecutor and investigator resources together from all three levels of law enforcement, CATCH has been able to lessen the jurisdictional problems and maximize the efficient use of investigators' time. Perhaps the most demonstrable evidence of CATCH's success is that no agency has withdrawn from the task force despite substantial resource commitments, so the participating agencies must believe CATCH has been a worthwhile endeavor. If a jurisdiction were considering starting a task force, visiting CATCH to observe its operations and

obtaining the MOUs and protocols would be very beneficial. Nor should a jurisdiction be deterred by the fact that CATCH's success has led to substantial growth in the size of the task force. (CATCH started out as only five-person task force only five years ago.)

The Lake County SAO has taken a different approach, which is harnessing the energies of a very dedicated small group comprised of a prosecutor, investigator, and digital evidence analyst to investigate and prosecute telecommunications fraud and assist the law enforcement agencies within the jurisdiction. The Lake County SAO uses its membership in a larger task force to alleviate some of the jurisdictional and manpower difficulties inherent in telecommunications fraud investigations. Similar to CATCH, the Lake County SAO's establishment of a multi-disciplinary team yields dividends in efficiency and allows the Lake County SAO to have an impact greater than the size of its assigned personnel. The drawback is that, much like a small business, there are no safety nets or fallback resources.

The Brunswick County DAO, with access to the least amount of resources, particularly for digital analysis, has experienced great difficulty in overcoming the jurisdictional and labor-intensive hurdles posed by telecommunications fraud investigations. Notwithstanding the difficulty, the jurisdiction has persevered to achieve justice on behalf of victims—particularly in the area of victim assistance, with a comprehensive victim notification system and a commitment to obtaining restitution. In addition, the Brunswick County DAO works with victims to help them work through injuries to credit ratings caused by telecommunications fraud.

Telecommunications fraud has been increasing and will only continue to do so as perpetrators take advantage of the anonymity of the Internet and telephone lines to steal money from consumers. If a jurisdiction is not already making an effort to address the problem, chances are it will soon have to do so. Based on the experiences of CATCH, the Lake County SAO, and the Brunswick County DAO, jurisdictions may want to consider the following issues in establishing their own efforts:

- formulate a clear mission statement for the effort;
- establish concrete, achievable goals;

- form partnerships with other law enforcement agencies that are consistent with the mission and goals of the effort, and consider involvement of private partners;
- provide incentives to encourage long-term commitment of participants to the effort;
- look for potential outside funding sources for the effort and be cognizant of the possibilities of in-kind contributions such as detailing personnel, providing equipment or office space;
- examine the feasibility of establishing a multi-disciplinary team comprised of a prosecutor, investigator, digital evidence analyst, and victim-witness assistance coordinator;
- consider investigative protocols that minimize investigative effort in producing relevant evidence;
- establish law enforcement and public education efforts to ensure that the law enforcement community is aware of the effort and to help prevent the public from being victimized; and
- periodically reexamine the mission, goals, make-up, funding, and workload of the effort to improve efficiency and make an impact on telecommunications fraud in the jurisdiction.

American Prosecutors Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, Virginia 22314
Phone: (703) 549-4253
Fax: (703) 836-3195
http://www.ndaa-apri.org

APRI