CHAPTER 1

"REAL WORLD" CASES: SOLVED AND UNSOLVED

The following four identity theft cases are examples of investigations conducted at the Identity Theft Crime and Research Lab at Michigan State University. To protect their anonymities, the names of individuals and their addresses have been changed; any resemblance to actual names or addresses is coincidental. These cases reveal some of the processes involved in identity theft investigations and also provide an insight into the ease with which some cases can be resolved while others may never be. This book is based on practical experiences learned from investigating these and hundreds of other identity frauds. The overriding goal is to provide business fraud investigators and victims themselves with tools for investigating identity theft cases. Law enforcement investigators, particularly those new to conducting investigations on the Internet, may also find this book useful. Beginning with Julie Ann Blakely, the cases dealt with some of the common types of identity thefts and describe steps that were taken to resolve them.

THE JULIE ANN BLAKELY CASE: INCARCERATION FRAUD

The call from the victim came into the Identity Theft Crime Lab on Thursday, December 16, 2004, at 9:30 A.M. Julie Ann Blakely had applied for a job at Belmont Hospital and was denied employment because of her criminal record in Detroit, Michigan. Julie claims to have never been involved in any criminal activity. The police will not help her. Would we?

Our first step was to determine whether Julie was actually a victim or was masking as one, which happens with increasing frequency as perpetrators find new ways to avoid detection of frauds they commit. To verify Julie's authenticity as a victim, we first went to the Detroit courthouse to search for any court records on "Julie Ann Blakely" and discovered that she, purportedly, had appeared in traffic court on six different occasions.

The second step was to conduct an Internet search of the records of offenders from the State of Michigan Corrections Department, using that state's public domain search system and the keyword "Blakely." The search revealed the name, date of birth, racial identification, gender, hair, and eye color, height, and weight, arrest, and incarceration records of a perpetrator with the last name of "Blakely," a list of aliases that included the names "Julie Blakely," "Julie Blake," and "Charlene Smith," and a photo of this offender who had recently been incarcerated. The photo was not a picture of the Julie Ann Blakely who had come to our crime lab for help.

The third step, therefore, was to arrange a meeting with Julie and the police officer whose name was on the court records as having apprehended her for a traffic violation. In the meeting, the officer described the incident in which, on September 10, 1999, a driver he had stopped for a traffic violation gave her name as "Charlene Ann Smith." A search of the police database, however, showed that no such person existed. The driver, therefore, after being issued citations for using improper plates, interfering with a police officer, having false ID, possessing drug paraphernalia, and having no operator's license and no valid

proof of insurance was processed and booked under the name of Jane Doe. She served 10 days in the jail at the Detroit Police Department.

Of particular note, however, was that while in jail, "Jane Doe" required medical treatment for a diabetic condition; she was admitted to a local hospital, where she admitted her name was not "Charlene Ann Smith" but, rather, was "Julie Ann Blakely"—the name imprinted on a medical card she had in her possession at the time of arrest.

Because of her incarceration, Charlene Ann Smith alias Julie Ann Blakely had been fingerprinted. We now had the following evidence to clear the real Julie Ann Blakely from crimes she did not commit: (1) DNA evidence (the fingerprints), (2) the photo of the since imprisoned Charlene Ann Smith who used the alias Julie Ann Blakely, and (3) the police officer's recognition that the person he arrested matched the photo we had obtained of the now imprisoned Charlene Ann Smith and that Julie Ann Blakely did not fit the description on the arrest report. The case, however, despite this evidence, could not yet be closed—Julie's criminal records would first have to be cleared.

Because of the charges, Julie now had a criminal history, which may be difficult to erase owing to the bureaucracy of government agencies. We, therefore, carefully documented every detail about the case to provide evidence that would clear the driving suspension recorded with the Secretary of State and the Bureau of Driver & Vehicle Records, the outstanding liabilities for debts incurred as part of the court hearings and processing, and the criminal records maintained in the databases of the Michigan State Department of Corrections and the Detroit Police Department.

We sent the documents of evidence, through U.S. certified mail so as to confirm their deliveries, to the personal attention of the directors of each government agency. We also sent copies of all the documents to each of the judges who had fined or sentenced "Julie Ann Blakely" on different occasions as well as to the Chief Judge of that district's court. The cover letters requested the judiciary to ensure that all records of court hearings and violations would be reversed and purged from the criminal databases.

Finally, we sent copies of all the documents to the Department of Human Resources, Belmont Hospital. Julie Ann Blakely, a 21-year-old single mother, was hired for the job for which she had applied at Belmont Hospital, she regained her driving privileges, and was, eventually, resolved from crimes she had never committed. Julie did not incur any great financial losses; the emotional costs, however, were immense and remain to this day.

Several lessons can be learned from this investigation: first, police departments may lack the resources to investigate or spend much time on some identity theft cases; second, some cases are easily resolved with simple strategies and detailed documentation; third, criminals impersonate others not only to commit crimes but also when they are apprehended (and most eventually are); fourth, the Internet is an important tool for identity theft investigations—in this case, it provided the key evidence; fifth, to circumvent bureaucracies, correspondence should be sent to the government officials personally; and sixth, documents should be sent using methods that will confirm receipt. This case illustrates that the process is not difficult; the investigation required only a plan of action that almost anyone could perform. The next case, also using the Internet as a tool could not, unfortunately, be solved.

THE RAY C. LAPIER CASE: SHIPMENTS TO ROMANIA

Unless there is clear evidence for organized crime, in which case federal law enforcement agencies will become involved, identity theft cases involving foreign countries are difficult to investigate and nearly impossible to solve. The best one can do is to help prevent further abuse of the victim whose identity was stolen and also of the merchant where merchandise or services were fraudulently purchased. Victims, nonetheless, sometimes wish to pursue the perpetrator, despite the odds against any apprehension. This is one such case.

On October 10, 2002, Ray C. Lapier received a telephone call from the fraud department at his Visa Credit Card Company. Had he authorized

the use of his Visa Signature Rewards card for a shipment of merchandise to Romania?

Perhaps not coincidentally, two weeks earlier, Mr. Lapier had taken his family on a weeklong cruise with the "ACME" Cruise Lines, where many employees are Romanian. Before contacting our crime lab, Mr. Lapier had already filed a complaint with the local police department. The police officer referred the case to us for investigation—the MSU Crime Lab collaborates with local and also federal law enforcement agencies on identity theft cases (when we collect sufficient evidence for a subpoena, search warrant, or arrest, the case is returned to the police officer for further action). In this case, Mr. Lapier wanted to know who his impersonator was, a concern common to most victims of identity theft.

In fact, with few exceptions, the majority of victims express a pressing need to know who their impersonators were. Many victims suspect their coworkers. Others may not point to a specific person but may claim to know the location where the identity theft had happened, often citing the workplace as the source of the theft. Regardless of who stole the identity or where it was stolen from and even when losses are negligible, most victims want to know the identity of their abusers.

Unfortunately, while stolen identities can be secured from further criminal use, at least temporarily, the offenders are difficult to track because, in most cases, the direct thief is a member of a larger, more or less organized, identity theft network in which crimes are "layered" so that only the front criminals are caught. These are the members of the network's cell who are responsible for opening postal boxes, renting apartments, or locating vacant houses for the deliveries of fraudulently ordered merchandise.

Once delivered to these locations by UPS, FedEx, or U.S. Mail, members of a second cell retrieve and transfer the merchandise to members of yet a third cell, who market the merchandise on the street. It is because of this network structure in which many perpetrators are intentionally involved in different aspects of the identity frauds that the leaders of the cells usually remain unknown—to both the police and also to the cell's members at lower levels of the network. (Identity theft

networks are further discussed in Chapter 2.) A given perpetrator, therefore, may be only the front person and not the organizer of the network.

Mr. Lapier was persistent. Prior to visiting the MSU Crime Lab, he had already taken the first step: the placing of "fraud alerts" on his credit files at each of the four credit reporting agencies—Experian, Equifax, TransUnion, and Innovis. (Innovis is a data broker—a seller of personal identifying information; so are the other three credit agencies. Innovis, as do the other three agencies, maintains and provides businesses with credit reports, but the U.S. Federal Trade Commission identifies only the first three as credit reporting agencies.) Merchants who wish to verify the name and creditworthiness of a prospective customer will contact one of these agencies, which maintain financial files on all or most U.S. citizens. The fraud alert on a financial record warns the merchant of the possibility of an impersonator.

The next step to be taken in this case was ours, and that was to obtain information from the fraud investigator at the credit card company. In the past, fraud investigators rarely gave any information to the victim and many still do not, despite the Fair and Accurate Credit Transactions Act (FACTA) that requires them to do so (see Chapter 5). At the time of this investigation, however, FACTA had not yet been enacted. In Mr. Lapier's case, we sought the following information: (1) the authenticity of the credit card charge, (2) the amount of the charge, (3) the type of merchandise that was fraudulently purchased, (4) the method of purchase, that is, physical store versus business Web site, (5) the name given by the purchaser, and (6) the address given for the delivery of the merchandise. This information is important for the following reasons.

Even when we have a copy of the credit card statement showing the amount of charge, it is necessary to verify the authenticity of a claim of identity theft.

Second, the Federal Bureau of Investigation should be notified of fraudulent transactions when the amounts are in the $50,000 range or more.

Third, the type of merchandise purchased provides clues, such as the gender of the offender and the extent to which the crime is organized. For example, discount store purchases of ladies' and children's clothing, cookware, and household items suggest a crime of a different nature as compared to purchases of expensive cameras, video, computer, and other technological equipment that are known to be sold in the black market, often to obtain cash to support a drug habit or to fund some other criminal activity.

Fourth, the method used to make the purchase can reveal the offender's identity. If the merchandise was purchased in a physical store versus an online Web site, video cameras positioned inside or outside may have captured the transaction or the license plate number and description of the getaway car. If the purchase was made online, Internet addresses can be traced (Chapters 9 and 10).

Finally, the address given on an application for the delivery of merchandise is where surveillance will be conducted to identify the front person whose task is to retrieve the fraudulently ordered merchandise. The delivery point is the end of the trail, the place where most identity theft investigations begin. This is because the crime scene—the place where the identity was stolen—is rarely known and so is the person who stole the identity that facilitated the identity fraud—the fraudulent purchase of merchandise.

The Visa company investigator was cooperative and so was the fraud investigator for L.L.Bean, the company where the credit card order was placed—for a pair of $105 men's shoes. (The police would not investigate this $105 crime; many police still do not recognize that this type of small offense may be a test of the system and tied into a larger network operation.) Clearly, the sole purpose of the pursuit by Mr. Lapier, as with most victims, was to find and bring to justice his impersonator.

We learned the following: an Anghel Castnel, or someone using that name, placed an Internet order on the Web site of the L.L.Bean Company for a pair of men's shoes costing $105 to be delivered to a person with the same name at Peniei-AL-7-BL-PA-11, 6000-L-BACAU, Romania. Further, the Internet e-mail address that was used to place

the order, using a credit card number issued to Ray C. Lapier, was CNEL_8@Yahoo.com.

With this information, we planned a specific approach, or strategy. The first step was to conduct Internet searches (the Internet is a valuable tool and a major focus of this book) to verify the name and address listed on the purchase form. The first search for the name "Anghel Costel" using smartpages.com (*www.smartpagers.com*) proved unsuccessful. The next search, using the Yahoo's People Search directory, was for the e-mail address that was used to place the order. We also searched the Yahoo Member Directory (*www.members.yahoo.com*). The Yahoo Member Directory search uncovered no information, but the Yahoo.com e-mail search revealed two addresses listed for an Anghel Castnel, both in Romania.

We furthered searched the white pages of several Romanian phone directories (*www.whitepages.ro*) and the addresses associated with the name Anghel Castnel. This search provided one address for Bacau, which was the name of the city given by the perpetrator when completing the online purchase form. Someone by the name of Anghel Castnel was registered as living in an apartment located at the address in Romania where the merchandise was shipped. In steps two and three we (1) contacted the cruise line and also (2) the Romanian police.

A cruise line employee with the last name of Castnel may have had access to the personal information of passengers; this individual could have made the fraudulent purchase for shipment to himself or to a family member with the same last name. The U.S. certified letter to the "ACME" Cruise Lines, inquiring whether an Anghel Castnel or someone with the last name Castnel had worked on the cruise ship during the dates that Mr. Lapier and his family were aboard, or whether someone with that name had, at any time, been employed in any job position with the company, was never acknowledged.

We sent a copy of the chain of evidence we had obtained, together with all documentation of the searches, including a copy of the police report and the detailed notes from conversations with the fraud investigators, to the Romanian National Police Force. To this date, we have received no reply.

What effectively did we do in this case? This investigation may only have served as a catharsis for the victim; perhaps the cruise line took steps to secure their passenger's personal information; possibly they also extended our investigation with one of their own, and, maybe the Romanian National Police did, after all, follow up.

Regardless of the outcome, however, this example of an actual case illustrates several aspects of identity theft investigations. First, as in the Julie Blakely case, emphasis is placed on the importance of developing a plan, or strategy, before going forward with an investigation; second, the Internet was, again, a valuable tool for verifying the name and address of the shipment—the end of the trail where, as pointed out earlier, most identity theft investigations must begin; third, the case demonstrates the importance of careful and detailed documentation that may be used by others ultimately involved in the investigation, for example, the cruise line or the Romanian police.

Finally, this case shows that, despite their expressed needs for such information, the victims may never know their perpetrators, particularly when the case crosses foreign boundaries (i.e., legal jurisdictions). Victims report, however, that any investigation of ones' case serves as a catharsis, regardless of the outcome.

THE JANICE A. MACKLIN CASE: THE VICTIM WAS THE PERPETRATOR

Janice A. Macklin was a victim of identity theft: her former husband, who was then living in another state, was using her name and also had access to and was using her Internet addresses (Internet Protocol and e-mail) to commit auction fraud on the eBay Web site. Ms. Macklin first learned of the fraud when the eBay company closed her account owing to fraudulent transactions. Ms. Macklin had targeted her husband as the likely suspect because (1) he knew she had a registered eBay account and (2) he had previously been convicted of embezzlement.

Prior to contacting the MSU Crime Lab, Ms. Macklin had contested eBay's closing of her account and had also filed a complaint with the

local police. The police, however, indicated they would not investigate this case. "Would we?" asked Ms. Macklin.

In addition to a voluntary background check and prior to opening a fraud file on an identity theft case, the Lab's standard procedure is to conduct a review of the victim's credit reports, which the victim obtains from each of the four credit reporting agencies—Experian, Equifax, TransUnion, and Innovis. Credit reports contain "red flags" for identity theft (discussed in Chapter 6), and, although infrequent, perpetrators have been known to use their own names to commit online frauds, claiming (when they are caught) that they are the victims of some impersonator who has stolen their identities and is using them. There is no objection, in our experience, by real victims to our background reviews; most victims, in fact, request that the reviews be conducted quickly so that the investigation can begin.

One "red flag" when reviewing a victim's credit reports is when sections or pages are missing or crossed off. Missing or crossed-off sections raise the question as to why the pages are modified —which raises the question as to whether information may have been omitted, either inadvertently or intentionally; if intentional, another question is "why?" Missing sections may contain aliases, addresses, or other information inconsistent with what a victim provides during the routinely conducted in-take interview. The routine check of Ms. Macklin's credit reports revealed missing pages, Ms. Macklin offered different explanations when questioned on two different occasions about the missing sections, and she failed to follow through on our repeated requests to provide the missing pages. The background check showed that Ms. Macklin uses, or at some time had used, several aliases; the report also revealed prior convictions for relatively minor traffic offenses. The report showed no theft or fraud-related arrests.

In cases such as this, where information obtained on a victim during the preinvestigation phase, or information provided personally by the victim, is inconsistent or questionable with what we know about identity theft (e.g., the use of alias names), the Lab procedure requires us to

establish the reliability of the victim's responses to information given during the intake part of the process. Reliability is estimated by conducting two independent interviews by two different investigators who use the same questions, reframed, and randomly ordered. The interviews may involve only a few questions to clarify inconsistencies, and they may be conducted either in person or over the telephone.

Ms. Macklin's responses were inconsistent, both to questions about the missing credit history information and also the chain of events involving the auction fraud. Also of questionable accuracy was the claim by Ms. Macklin that her husband was able to access and use her Internet address. We, therefore, pursued further verification on details of the case.

The eBay fraud department cooperated. We learned that, on five different eBay auctions, a Janice A. Macklin had sold Playstation systems and accessories; the winners paid for their purchases through an online bank transfer system whereby money is automatically transferred from the bidder's bank account to the account of the eBay seller. In all the five cases, the bidders had paid the seller but, in return, had received no merchandise. With this information, we contacted the police department where Ms. Macklin had filed her identity theft complaint.

Although initially he had informed Ms. Macklin that her case could not be investigated owing to departmental understaffing, the police officer now sought and, subsequently, obtained a warrant to search the premises for identity theft impersonation evidence, namely, Playstation systems and accessories, and a computer that could be analyzed. The search produced the evidence, and the Internet Protocol (IP) and e-mail addresses traced to the computer located in Ms. Macklin's residence. Confronted with the evidence, Ms. Macklin admitted she was the perpetrator and not the victim; she was fined, ordered to pay restitution, and placed on probation.

What can be learned from this investigation? First, there are, indeed, perpetrators who claim to be victims; second, the routine background information obtained on a victim's claim can point to "red flags"; third, routine questions asked by two different interviewers at two different

points in time concerning inconsistencies in background information can help establish the reliability of a victim's responses; fourth, cooperative fraud departments can provide the necessary evidence to pursue the investigation further; and fifth, under-resourced police departments, given sufficient evidence, can bring a case to closure. In the present case, Ms. Macklin claimed to be the victim; in the next case, the victim was charged as the criminal.

THE MARIA G. LOPEZ CASE: A CRIME OF FORGERY

The Lopez family was celebrating the Christmas holiday in the festive, traditional fashion of their beloved Mexico. Now, however, the Lopezes lived in the midwestern United States, where in the wintertime the wind chill was 20 degrees below zero and the snow knee-deep. Mr. and Mrs. Lopez had secured good employment, and their children, Maria and Juan, had been accepted into the university. Their long-held dreams had come true. Moreover, the Lopez family had found a little three-bedroom house in a neighborhood where the residents took pride in their modest, well-maintained homes and manicured lawns. And now it was Christmas. This meant that as many as possible of the Lopez's extended family—or as many as could (or would) come to this cold climate—would gather together for a weeklong celebration.

It was during dinner on this Christmas Day that Officer Montange knocked at the side door. The Lopez family—aunts, uncles, cousins, and Grandma Lopez—were all seated around a long table in the big, warm kitchen, chatting and laughing, and enjoying the meal and each other's company. Honored by the thought that a police officer had taken the time to come to his home on Christmas Day to return Maria's purse stolen so long before, Mr. Lopez, without a moment's hesitation, invited the officer to join them—they would make room around the table and there was plenty of food. They would "set another plate."

But the officer had no purse to return; he came instead to arrest Maria Lopez for the crime of forgery. In front of her parents, grandmother, and other relatives, Maria was handcuffed and taken away in the patrol car;

arrested on Christmas Day, in her new country, for a crime she claimed she did not commit. The entire Lopez family was in shock.

The case history is shown in Exhibit 1.1.

EXHIBIT 1.1 *Maria Lopez Case History*

February 2004	Maria's purse containing driver's license and bank card stolen while checking out books from main university library.
March 9, 2004	Hispanic female identified by driver's license as Maria Lopez rents video game systems, games, and movies from video store.
March 19, 2004	Maria Lopez (purported impersonator) fails to return video store game systems, games, and movies. Manager contacts the company's other video stores to red flag the name "Maria Lopez." Manager discovers open accounts at each store, in the name of Maria Lopez. Manager tracks down Maria Lopez at the address on the rental form, which was taken from the driver's license. Maria Lopez (the victim) goes to the video store, explains to manager that her purse had been stolen, and claims her innocence. The manager recognizes that Maria Lopez (the victim) was, indeed, not the person who had rented the video equipment; manager then verifies error by comparing Maria's handwriting with the signature on the rental agreement.
March 21, 2004	Maria's (the victim) father now takes her to police station to file report on stolen purse and report the fraud incident.
March 21, 2004	Police department places a "red-flag alert" on Maria's driver's license record.
April 12, 2004	Manager of video store contacts police department to report a larceny of video game systems, games, and movies by someone impersonating another person. Manager's statement on police report: "The suspect must resemble Maria Lopez to some degree."

(continued)

EXHIBIT 1.1 *(continued)*

June 29, 2004	Hispanic female, identified by driver's license as Maria Lopez, attempts to cash a $900 check at a discount store. Suspicious cashier buzzes security who, in turn, calls police. Suspect hurriedly leaves store without driver's license or check, and drives out of the parking lot. Security gets vehicle description but not plate number. Cashier identifies the image on the driver's license as the person who presented the check. Police take check and driver's license and place them into evidence at police department.
August 15, 2004	Police officer attempts to contact Maria at residence given on driver's license; Mrs. Lopez (Maria's mother) believes officer is there about Maria's stolen purse, but Maria is in Texas; Mrs. Lopez gives officer telephone number to reach Maria in Texas.
August 15, 2004	Mrs. Lopez calls Maria in Texas about visit from police officer; Maria telephones police department, leaves name and telephone number for officer to return call. Officer does not return call.
September 10, 2004	According to police statement, officer drafts letter to Maria Lopez asking her to come in for an interview. The report states: "Suspect did not respond."
October 22, 2004	Officer contacts the prosecutor's office to obtain a subpoena. Subpoena to obtain check number and other information about the check goes out to the financial institution named on the check. Results reveal the check was fraudulently manufactured.
November 26, 2004	Officer contacts discount store; views videotape of suspect at counter attempting to cash check; security officer advises that the subject in the video is same as image on driver's license.
December 25, 2004	Maria Lopez is arrested at her home for forgery and attempt to use false document to obtain $900; Mr. Lopez (Maria's father) follows police car to jail; arranges to post bail; meanwhile, Maria is locked in jail.
January 12, 2004	Maria, out of jail on bail, makes appointment to meet an identity theft investigator at the MSU Identity Theft Crime and Research Lab.

EXHIBIT 1.1 *(continued)*

January 13, 2004 MSU investigator conducts routine background check and interviews Maria; requests copies of police reports, including the report made of her stolen purse as well as documents showing that a red flag was placed on her driver's license, and the name and address of video store manager. Investigator makes appointment with security to view discount store video.

January 14, 2005 Two MSU investigators, Maria Lopez, and security officer view video at discount store; video shows Hispanic female with long black hair, just like Maria's; the female, however, is taller than Maria. The female is pregnant.

January 15–17, 2005 Further investigation by the MSU Lab investigators revealed the following information:

- The discount store video of the person attempting to cash check showed only a side view; there was no frontal view to show the person's face.
- The security officer admitted to the Lab investigators that neither the check nor driver's license was preserved for fingerprinting; both check and license were handled several times by the cashier, the police officer, and the security officer.
- The video manager confirmed to the Lab investigators and Maria that the only common feature between the person who had rented the equipment and Maria was that both had long, black hair.
- The police acknowledged that they failed to see the "red flag" placed on Maria's driver's license record in March 2004.
- The security officer confirmed to the Lab investigators that the video of the female who had attempted to cash the check showed that she was obviously pregnant.
- Maria is not pregnant now, nor has she ever been pregnant.

(continued)

EXHIBIT 1.1 *(continued)*

Tues., Jan. 25, 2005	Maria appeared in district court for the preliminary hearing. Based on the above evidence together with notarized documents from both the video store manager and the security officer, Case Number 04-1973—Maria Lopez, ". . . was adjourned by the authority of the judge for good cause shown."

The perpetrator in this case has yet to be apprehended; now, however, largely because of the time and efforts of the investigators at our Identity Theft Lab, Maria's name has been cleared from the state's criminal databases—for crimes she did not commit.

Although she lost no money and was convicted of no crime, the emotional costs remain considerable. For Maria, the anguish of the pain suffered by her parents and grandmother, and the embarrassment of being arrested and handcuffed in the presence of her relatives, remains, to this day, a source of psychological distress.

Maria's case and the others above are only four of many that, since 1999, have been investigated by the MSU Crime Lab. No two cases are alike; nonetheless, they all involve some basic, common methods and procedures, which is what these cases intended to portray. The background check before beginning an investigation, the reliability interviews for inconsistent information, the development of a strategy (which becomes modified as the investigation progresses) all have been emphasized. The following chapters elaborate on other common aspects, including the several chapters that emphasize and illustrate the importance of using the Internet and the computer as primary twenty-first-century investigative tools. First, however, before embarking on any identity theft investigations, it is essential that one knows the crime and understands the criminal.