EXPLORING METHODOLOGIES TO INVESTIGATE CROSS-BORDER IDENTITY THEFT
IN THE SAN DIEGO–TIJUANA REGION:
FROM POINT OF USE TO PERPETRATOR

By

Daniel Clift

A Capstone Project Submitted to the Faculty of

Utica College

December 2013

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in
Economic Crime Management
Abstract

The purpose of this project was to explore contemporary investigative methodologies to assemble a framework to effectively address cross-border identity theft cases in the San Diego–Tijuana region. This unique type of crime currently creates significant challenges for law enforcement in the world’s largest transnational metropolitan area. Cross-border identity frauds tend to be digital in nature with most schemes utilizing the Internet. Thus, suspect information is rarely available at the onset of an investigation and as a result draw little priority from criminal investigators. Available literature severely lacks investigative methods to address this rapidly growing consumer crime, particularly schemes that straddle the U.S./Mexico border. This project aims to fill that gap. Cross-industry research was completed to identify investigative techniques that could connect the point of use of a victim’s personal identifying information with the perpetrator responsible for the act. The findings of this research could be applied in numerous settings; however, this particular project caters to the border region of San Diego, California, and Tijuana, Mexico.

Keywords: Economic crime management, Raymond Philo, e-commerce, IP address tracing, data packet analysis, forensic e-mail analysis, data analysis, criminal networks
Table of Contents

List of Illustrative Materials ........................................................................................................ vii
The Identity Theft Epidemic in San Diego and Throughout the U.S. ........................................... 1
Definitions: Identity Fraud Versus Identity Theft ........................................................................... 3
Stages of Identity Theft ..................................................................................................................... 4
  Stage 1: Acquisition of personal information .............................................................................. 4
  Low technology methods of acquisition ....................................................................................... 5
  High technology methods of acquisition ...................................................................................... 6
  Stage 2: Point of use: Executing the offense .............................................................................. 8
  Bank account takeover .................................................................................................................. 8
  New account fraud ....................................................................................................................... 9
  Payment card frauds for existing accounts ............................................................................... 10
  Stage 3: Discovering and reporting the identity theft .............................................................. 10
Identity Theft Victimization ............................................................................................................ 11
Identity Theft in an Online World ................................................................................................... 13
  E-Commerce and Online Payment Systems .............................................................................. 14
  Online credit card transactions ................................................................................................... 16
  Alternative payment methods .................................................................................................... 16
  Payment aggregators .................................................................................................................. 17
  Mobile payment applications ..................................................................................................... 18
Mexico Embraces Cash Alternatives, E-Commerce, and Internet Banking .................................. 19
Cybercrime and Identity Theft in Mexico ....................................................................................... 20
Geopolitics and Cross-Border Travel ............................................................................................ 21
  San Diego and Tijuana: Interconnected Economies ................................................................. 22
Cross-Border Fraud: A Growing Concern for U.S. Border Regions ......................................... 22
  Understanding Border Security and Crossing Data ................................................................ 23
Law Enforcement Challenges With Identity Theft Investigations ............................................... 25
  Identity Theft Networks ............................................................................................................ 26
Analyzing Data Findings From the Literature Review ............................................................... 27
Research Methods ........................................................................................................................ 28
Research Findings ........................................................................................................................ 29
  Identifying Preliminary Investigative Leads ........................................................................... 29
  Investigative Techniques for Location Tracing ....................................................................... 30
Data Analysis: The Big Picture ..................................................................................................... 31
Exploring the Digital Footprint ..................................................................................................... 32
  Understanding Internet Protocol Addresses .......................................................................... 32
  Tracing IP Addresses ................................................................................................................. 33
  Connection ports ....................................................................................................................... 34
  Identifying specific devices ....................................................................................................... 35
  Limitations of IP Address Tracing ......................................................................................... 36
  Challenges of web proxies and anonymity applications ....................................................... 36
  Tor browser: Roadblock to traceability ................................................................................... 38
Tracing Online Activity Through Forensic Data Packet Analysis ............................................. 39
Digital Fingerprinting .................................................................................................................. 40
  Digital fingerprinting through WMH ...................................................................................... 40
Identifying the Source of a Data Packet Using WMH Values ..................................................... 41
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Packet Tracing Through PPM and Header Compression</td>
<td>43</td>
</tr>
<tr>
<td>Considerations With Virtual Private Networks</td>
<td>44</td>
</tr>
<tr>
<td>Application of Forensic Data Packet Analysis</td>
<td>44</td>
</tr>
<tr>
<td>Limitations of Tracing Data Packets</td>
<td>45</td>
</tr>
<tr>
<td>Forensic Examination of E-Mail Messages</td>
<td>46</td>
</tr>
<tr>
<td>Analyzing E-Mail Message Headers</td>
<td>47</td>
</tr>
<tr>
<td>Tracing E-Mail Messages to Their Source</td>
<td>52</td>
</tr>
<tr>
<td>Cell Phone Forensic Techniques for Cross-Border Identity Theft Investigations</td>
<td>53</td>
</tr>
<tr>
<td>Incorporating Mobile Phone Data into Investigations</td>
<td>54</td>
</tr>
<tr>
<td>Data Collection and Device Tracking</td>
<td>54</td>
</tr>
<tr>
<td>Identifying the location of a device</td>
<td>55</td>
</tr>
<tr>
<td>Triangulation</td>
<td>56</td>
</tr>
<tr>
<td>Combined tracking methods</td>
<td>57</td>
</tr>
<tr>
<td>Mobile Devices as a Source of Social Network Data</td>
<td>58</td>
</tr>
<tr>
<td>Mobile Phone Devices: Gateways to Information</td>
<td>59</td>
</tr>
<tr>
<td>Monitoring Wi-Fi Networks and Devices</td>
<td>60</td>
</tr>
<tr>
<td>Intercepting and Analyzing Electronic Communications</td>
<td>61</td>
</tr>
<tr>
<td>Keystroke logging</td>
<td>63</td>
</tr>
<tr>
<td>Traffic analysis</td>
<td>64</td>
</tr>
<tr>
<td>Legal Considerations</td>
<td>64</td>
</tr>
<tr>
<td>Overview of Wi-Fi Surveillance and Implementation</td>
<td>65</td>
</tr>
<tr>
<td>Making the Connection: Applying Data Analysis Using Link Diagrams</td>
<td>66</td>
</tr>
<tr>
<td>Analyzing Victim Transactions for Method of Acquisition</td>
<td>68</td>
</tr>
<tr>
<td>Linking IP Addresses</td>
<td>70</td>
</tr>
<tr>
<td>Analyzing Border Crossing Information</td>
<td>72</td>
</tr>
<tr>
<td>Analyzing Layered Schemes</td>
<td>73</td>
</tr>
<tr>
<td>Using Social Network Analysis to Unravel Identity Theft Networks</td>
<td>75</td>
</tr>
<tr>
<td>Social network analysis with call records</td>
<td>76</td>
</tr>
<tr>
<td>Cross-referencing suspects with call and text records</td>
<td>77</td>
</tr>
<tr>
<td>Centrality and hierarchies</td>
<td>79</td>
</tr>
<tr>
<td>Closeness and betweenness</td>
<td>80</td>
</tr>
<tr>
<td>The Importance of Data Analysis</td>
<td>83</td>
</tr>
<tr>
<td>General Recommendations</td>
<td>84</td>
</tr>
<tr>
<td>Addressing Cross-Border Identity Theft With a Holistic Approach</td>
<td>84</td>
</tr>
<tr>
<td>Partnering With Mexico</td>
<td>85</td>
</tr>
<tr>
<td>Practical Scenario 1: Hypothetical Scenarios</td>
<td>86</td>
</tr>
<tr>
<td>“Two free nights at a motel… with a gift card?”</td>
<td>86</td>
</tr>
<tr>
<td>The scheme</td>
<td>86</td>
</tr>
<tr>
<td>Possible solution</td>
<td>87</td>
</tr>
<tr>
<td>‘Give him credit’</td>
<td>88</td>
</tr>
<tr>
<td>The scheme</td>
<td>88</td>
</tr>
<tr>
<td>Possible solution</td>
<td>89</td>
</tr>
<tr>
<td>“Malicious funds transfer”</td>
<td>91</td>
</tr>
<tr>
<td>The scheme</td>
<td>91</td>
</tr>
<tr>
<td>Possible solution</td>
<td>91</td>
</tr>
<tr>
<td>Potential Framework for Success</td>
<td>92</td>
</tr>
</tbody>
</table>
Conclusion ................................................................................................................................. 93
References..................................................................................................................................... 95
List of Illustrative Materials

Figure 1 – Basic web proxy model ........................................................................37
Figure 2 – Data packet comparison .......................................................................43
Figure 3 – Sample AOL e-mail header ...................................................................48
Figure 4 – Trilateration example ............................................................................56
Figure 5 – Cell phone pinging using multiple signal sources .................................58
Figure 6 – Common transaction data ......................................................................69
Figure 7 – Identifying common IP addresses ...........................................................71
Figure 8 – Accumulated border crossing data ..........................................................73
Figure 9 – Transaction layering scheme ..................................................................74
Figure 10 – Location layering ..................................................................................75
Figure 11 – Cell phone contact list .........................................................................77
Figure 12 – Analyzing calls and text messages .......................................................78
Figure 13 – Sample hierarchy ..................................................................................79
Figure 14 – Complex identity theft network .............................................................80
Table 1 – Results of betweenness and closeness calculations .................................81
Figure 15 – Results of betweenness and closeness .................................................82
Figure 16 – Scenario 1 link diagram .......................................................................88
The Identity Theft Epidemic in San Diego and Throughout the U.S.

Identity fraud received national recognition in the early 1990s (Pontell, 2009). According to the Government Accountability Office (1998), estimated losses associated with identity theft totaled $442 million by 1995, increasing to $745 million by 1997. By 2003, the estimated costs to consumers and businesses exceeded $5 billion (Acohido & Schwartz, 2005). San Diego County was no exception as it experienced a rapid increase of identity fraud cases fueled by methamphetamine use combined with technological improvements that made information more accessible (Biegelman, 2009). Personal identifying information (PII) was readily available to those who knew where to look. As credit card networks expanded, corporations were handling higher volumes of personal information. Poor handling of records led to sensitive documents being discarded in trash cans and dumpsters, which would become a rich source of information for identity thieves and coin the term “dumpster diving” (Collins, 2006).

During the 1990s in San Diego, the U.S. Postal Service began using neighborhood delivery and collection box units (NDCBUs), to improve the efficiency of mail delivery by providing a central drop off point for clustered residences (Biegelman, 2009). Unfortunately, while the NDCBU did in fact reduce mail delivery times, it also provided a central location for identity thieves to steal sensitive personal information from numerous individuals. Counterfeit or duplicate master keys to NDCBUs gave offenders unimpeded access to mail drop-off points throughout San Diego, resulting in an area hit particularly hard by a rapidly expanding crime phenomenon of using another individual’s information for personal financial gain.

Early on, most identity thieves in San Diego were supporting methamphetamine habits (Biegelman, 2009). By 1994, San Diego topped the list of U.S. cities for methamphetamine use; local treatment centers reported patients seeking treatment for that drug more than all the others
Identity theft was attractive to substance abusers, since it was relatively easy to facilitate, non-violent, and difficult for law enforcement to investigate (Pontell, 2009). In fact, during the 1990s, law enforcement prioritized most other crimes above identity theft and in many instances did not investigate it at all (Biegelman, 2009).

The digital age also expanded the realm of identity theft, ushering in faster methods to obtain credit without ever entering a bank, providing large repositories of stored data to target for PII acquisition, and online payment methods to fraudulently use credit cards without having to come face-to-face with a merchant (Marshall & Tompsett, 2005). The rise of Internet banking provided opportunities for identity theft perpetrators to quickly make use of stolen personal information with the ability to apply for multiple credit cards and receive instant approval. Methamphetamine abusers frequently exploited the Internet to facilitate identity theft schemes, resulting in faster monetary gains as multiple transactions could be completed in a shorter amount of time (Acohido & Schwartz, 2005). As electronic payment systems expanded, both public and private entities began storing large volumes of sensitive consumer data. Technologically savvy computer hackers were able to systematically access vast quantities of information, resulting in identity thefts on the largest scales ever seen (Pontell, 2009).

Furthermore, online black markets provided a forum to sell and trade stolen credit card information or entire personal profiles, which could be used to execute a variety of identity theft schemes. Electronic commerce led to more faceless interactions between customers and merchants, opening additional opportunities for identity thieves to complete fraudulent transactions.
Definitions: Identity Fraud Versus Identity Theft

For the purpose of this study, identity fraud is defined as the misrepresentation of one’s identity for personal gain. Identity fraud includes the crime of identity theft, which is the acquisition of the personal identifying information of another with the intention of using it without authorization (Finklea, 2012). Identity fraud and identity theft are frequently used interchangeably, however, there are a few differences. Identity fraud includes the use of synthetic identification, or falsified information for the purpose of defrauding another (U.S Department of Justice, 2013). Identity fraud refers specifically to the misrepresentation of one’s identity, even though it includes the unauthorized use of another’s personal data. Some have specified identity theft as unauthorized access to personal information while identity fraud is the actual use (Gilbert & Archer, 2012). However, for this project both terms refer to the theft and use of personal data to commit fraud, which is simply misrepresenting material information for economic gain.

Section 530.5 of the California Penal Code lists the elements for an identity theft charge as follows:

Anyone who willfully obtains personal identifying information… of another person, and uses that information for any unlawful purpose, including to obtain or attempt to obtain credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense.

When a victim discovers their information was used by another for financial gain, they are generally considered a victim of identity theft. When a suspect misrepresents their identity to a business for personal gain, such as applying for credit with another person’s information, that entity is a victim of identity fraud (Gilbert & Archer, 2012). Not all identity frauds are committed for immediate financial gain. An individual may use another’s identity to avoid
detection of a crime committed or travel to a country in which they would otherwise be denied entry (GAO, 2008). This project focuses on schemes predicated upon some form of financial gain such as credit card fraud and bank account takeovers, which are the most frequent in the San Diego–Tijuana region.

**Stages of Identity Theft**

Regardless of how each particular scheme is perpetrated, identity thefts occur in three stages: acquisition of the victim’s personal or account information, using the information to complete the offense, and discovery of the crime (Newman & McNally, 2005). There are numerous methods to complete an identity theft scheme, including some that have yet to be discovered. The perpetrator’s choice of how to facilitate identity fraud directly influences law enforcement’s initial approach to the investigation. Law enforcement personnel at all levels should be expected to understand the basics of identity theft offenses in order to properly document them, even prior to the case being transferred to more specialized teams of investigators. An incomplete preliminary report by a police officer or duty agent could significantly hinder an investigation (Collins, 2006).

**Stage 1: Acquisition of personal information.** Identity theft begins with obtaining an individual’s personal identifying information (PII). This usually consists of name, birthday, social security number, individual tax identification number, or sensitive financial account numbers. A person’s name and birthdate are not kept entirely confidential, and alone would not be considered PII since it is possible for more than one person to share those same attributes. However, when combined with unique identifiers such as a social security number and other descriptive information such as an address and mother’s maiden name, one could assemble a full
personal profile, which could then be used to complete a credit card application or open a bank account.

Another unique identifier is an account number of a credit card or bank account. Credit card fraud is currently the preferred identity theft method in the San Diego region (Federal Trade Commission, 2013). A perpetrator who obtains a personal profile with a credit card number from an existing account will have a much easier approach to successfully completing an unauthorized transaction than someone who must create an entirely new account under the victim’s name (Mann, 2011). For any law enforcement investigator tasked with investigating identity theft offenses, it is helpful to understand the common methods used to obtain an individual’s information to assemble a personal profile.

Identity thieves use various methods to unlawfully obtain personal information. In some cases, personal profiles and stolen credit card numbers are sold or traded on the Internet black market (Zeller, 2005). Others could include mail theft, cyber intrusions, motor vehicle burglaries, or dumpster diving (Biegleman, 2009). When an identity fraud investigation reveals the method of acquisition, the full scheme can be described, which may connect the offender to other crimes or simply strengthen the prosecution of the current case. Identity thieves deploy different methods to acquire victim information with varying levels of sophistication (Rebovich, 2009). The method of acquisition can be categorized generally as high technology or low technology (Allison, Schuck, & Lersch, 2004).

**Low technology methods of acquisition.** Low technology methods include larcenies such as mail theft and burglaries as well as dumpster diving. Prior to the development of the Internet, mail theft was the preferred method to obtain personal profiles in San Diego County and remains a popular choice among identity thieves (Biegleman, 2009). Other common methods currently
used to steal personal documents in San Diego include burglaries to residences, businesses, and motor vehicles. In 2012, the city of San Diego reported 19,188 total thefts, including burglaries, vehicle break-ins, and basic larcenies (ARJIS, 2013). Employee thefts are also common, which occur when an employee has access to personal data, such as customer account information for a retailer, and uses the information for illicit personal gain. An even simpler method of acquisition involves taking personal items left unattended in public areas, such as purses and wallets.

Finally, one of the oldest low technology methods for obtaining personal identifying information is dumpster diving. This technique simply involves entering a dumpster or trashcan in search of documents that contain sensitive information that could be used to assemble an individual’s profile (Biegelman, 2009). Identity thieves who prefer low technology techniques to obtain an individual’s PII still utilize the internet to apply the information to an actual scheme, since the internet enables consumers to engage in user friendly e-commerce and internet banking applications (Marshall & Tompsett, 2005).

**High technology methods of acquisition.** High technology methods of acquisition include e-mail phishing scams, skimmers, network intrusions, and data breaches. E-mail phishing is a technique where an e-mail message appears to be an authentic correspondence from a legitimate company or colleague with a link or image that contains malicious software, or malware (Upendar & Rao, 2013). Once the recipient clicks on the link, the malware extracts sensitive information from their computer, such as passwords, Internet history, and stored documents and then sends that information back to the person who originally created the link. The perpetrator is then able to analyze passwords and web browsing history to access the recipient’s various financial accounts. In other instances, phishing e-mails simply request the recipient’s personal information, including bank account numbers, under the guise of needing
assistance to complete a large cash transfer (Bergiel, Bergiel, & Balsmeier, 2008). E-mail phishing schemes are among the fastest growing methods for committing identity fraud in the United States (Upendar & Rao, 2013).

Skimming devices copy payment card information stored on the card’s magnetic strip. These devices are frequently installed in credit card terminals at gas stations or ATM machines and surreptitiously record card information from each customer. Often, a small hidden camera will accompany the device to record an associated PIN number (Moore, 2011). The recorded information from the magnetic strip is then used to clone the payment card or simply make Internet purchases with the card number.

Large scale identity theft schemes are often facilitated through data breaches, which include accessing a computer system without authorization for the purpose of sensitive data exfiltration (Moore, 2011). Consequently, an individual hacks into a computer system that contains large volumes of sensitive data, such as customer credit card numbers, extracts the information, and then uses it to commit numerous identity theft offenses. The largest identity theft scheme to date resulted from the TJ Maxx data breach, where hackers stole about 47.5 million credit and debit card numbers over two years. Some estimate that the perpetrators stole up to 200 million card numbers (Brightman, 2009). Data breaches may also occur through network intrusions. Unsecured Wi-Fi networks are vulnerable to unauthorized access by people within close proximity to the connection ports or access points. Once someone is on the network, they are able to view information being shared (Reyes, O’Shea, Steele, Hansen, Jean, & Ralph, 2007).

If investigators are able to determine how the suspect initially came into possession of the victim’s information, they could use that information to connect the suspect to a criminal
network, unsolved cases, or simply assemble a more complete indictment. However, it may not be immediately known how the suspect obtained the victim’s information, and investigators should understand that acquiring that knowledge is not always necessary to successfully investigate the transaction and satisfy the elements for prosecution. Rather, identity theft investigations focus on the information that is readily available, which are the details surrounding of the point of use of the victim’s PII since which contain clues to trace the transaction to a perpetrator.

**Stage 2: Point of use: Executing the offense.** Once PII is obtained, it is relatively easy to use to carry out the identity fraud scheme. Applications for new credit card accounts can be completed online or existing ones can be used to purchase items in stores or through e-commerce payment systems. The processes are designed to be very user friendly, so even the unsophisticated offenders who extract sensitive information from dumpsters can log onto a public Wi-Fi network and, within minutes, complete numerous credit card applications with the victim’s information. Even if the perpetrator is limited to one transaction before the card issuer or bank freezes the account, the victim may not be entirely safe. A personal profile could be used to obtain additional accounts (Newman & McNally, 2005). Repeat victimization demonstrates that prevention alone will not stop an identity thief, fueling the argument for an effective law enforcement response. Below are a few of the most common identity fraud schemes experienced in San Diego, California.

**Bank account takeover.** Bank account takeovers are among the most damaging types of identity frauds for businesses and consumers. An account takeover occurs when a perpetrator assumes control of an existing financial account, usually a bank account such as checking, savings, or money market, gaining direct access to the accountholder’s funds (Newman &
McNally, 2005). Other types of accounts that may be targeted include brokerage or line of credit. The fraudster needs to acquire enough information to access the account, such as account number, routing number, and password for electronic access. These are considered identity fraud crimes since the offender is impersonating the account holder, disguising the activity as legitimate. Bank account takeovers can be devastating to victims. Unlike credit card accounts where charges can be disputed and credit can simply be returned to the victim’s account, a complete takeover of the victim’s bank account allows the perpetrator to remove all of the available funds, resulting in direct financial devastation. Since this type of scheme has a more noticeable effect, victims are more likely to report cases of bank account takeovers to the police (Mann, 2011).

**New account fraud.** New account fraud involves opening a financial or utility account using another individual’s personal identifying information. New account frauds most commonly involve credit cards (Sullivan, 2010). For example, a perpetrator uses a victim’s PII to complete an application to obtain a credit card in the victim’s name. The perpetrator could then complete numerous purchases or cash advances while the debt and liability is assigned to the victim. New account frauds tend to take the longest to discover, with an average of six months (Newman & McNally, 2005). New account fraud can cause the most damage to a victim’s credit score and require months to recover (Collins, 2006).

New account frauds also include obtaining a loan under the victim’s name. Loan fraud is tempting for perpetrators since a large sum of money is dispersed rather than smaller amounts, which are more typical for cash advances (Biegelman, 2009). With the expansion of Internet banking, applications for new accounts are readily available online with instant approval.
(Pontell, 2009). During 2012, identity frauds involving new accounts were reported in California at nearly twice the rate of existing accounts (Federal Trade Commission, 2013).

**Payment card frauds for existing accounts.** Payment card frauds for existing accounts result in billions of dollars in losses globally each year (Barker, D’Amato, & Sheridon, 2008). In the United States, credit and debit card fraud were among the most common types of identity thefts reported to the Federal Trade Commission (FTC) in 2012 (FTC, 2013). Upendar and Rao (2013) noted from their consumer survey, that people perceived identity theft from credit and debit card fraud as a number one fear because of a lack of prevention and frustration with deterrence. The volume of identity frauds involving existing payment cards is significant, especially in transnational schemes considering over 59 billion payment card transactions occurred throughout the global economy in 2009 (Upendar & Rao, 2013).

**Stage 3: Discovering and reporting the identity theft.** Victims are usually notified once their information has been used to attempt or complete a fraudulent transaction. Generally, law enforcement does not become involved until after the crime has occurred and the victim or financial institution decides to file a police report. The discovery of identity theft schemes involving the unauthorized use of a victim’s credit card generally occurs shortly after the transaction (Barker, D’Amato, & Sheridon, 2008). However, more complex schemes such as account takeovers or using a victim’s information to open new credit accounts may take longer to discover. Research shows that the amount of time that passes before discovering the crime is related to the amount of financial loss suffered by the victim (Newman & McNally, 2005). Fortunately, new legislation such as data breach notification laws has increased the awareness and prevalence of reporting identity thefts and assisted with retracing potential points of information acquisition for suspects (Romanosky, Telang, & Acquisti, 2011). Absent of a data
breach, it can be difficult to retrace the initial method of acquisition, considering all of the potential methods available to perpetrators.

To summarize, preliminary reports made to law enforcement should document at least stages two and three of the identity theft scheme. The point of use, which involves the actual transaction or credit obtained, will contain the most details to commence an investigation. Even if the method of acquisition for the victim’s information is unknown, proof that another individual possessed the information and then either attempted or completed a transaction needs to be documented to confirm that a crime occurred. Also, the specific method of discovery, whether notification from a bank official or credit card issuer or simply reviewing a credit report, should also be noted in a preliminary police report as a starting point for the more in-depth investigation that will follow (Collins, 2006).

**Identity Theft Victimization**

Statistics in relation to identity theft offenses illustrate the widespread victimization and cost to consumers. The Bureau of Justice Statistics reported over 11 million people, or over 5% of the U.S. population age 16 or older, experienced at least one type of identity theft during a 2-year period, resulting in a total financial cost of nearly $17.3 billion (Langton & Planty, 2010). According to the Bureau of Justice Statistics (2011), 7% of households nationwide, or about 8.6 million, reported having at least one victim of identity theft in 2010. Approximately 42% of identity theft victims spent one day working to resolve their resulting financial and credit problems, while 3% continued to experience issues related to the theft for more than six months after their initial discovery (Langton & Planty, 2010). Data indicated that the most common identity thefts involved the unauthorized use of a credit card or other type of existing financial account. The unauthorized use or attempted use of a credit card was not only the most common
type of identity theft, but increased at an alarming rate, from 3.6 million reported incidents in 2005 to 5.5 million by 2010 (Langton, 2011). During 2010, households that reported the misuse of other types existing accounts such as checking, savings, or PayPal reached about 3 million and 16% of households reporting such victimization suffered a loss of at least $1,000 (Langton, 2011). Identity theft has affected households throughout the United States, including high percentages in California.

In 2007, the Federal Trade Commission (FTC) received 43,892 identity theft complaints from California residents, with financial losses resulting from fraud and identity theft exceeding $171 million (FTC, 2008). In the San Diego metropolitan area, 3,509 incidents of identity theft were reported to the FTC in 2007, which translated to approximately 119 victims per 100,000 residents (FTC, 2008). In 2012, the FTC received a total of 46,358 identity theft complaints from consumers in California. Of those complaints, over 25% involved credit card or bank fraud (FTC, 2013). The most common bank fraud offense was unauthorized electronic funds transfers, where the perpetrator simply transferred money from the victim’s account into their own (FTC, 2013).

While real property crime statistics in San Diego far exceed identity theft offenses, these crimes can cause significant harm to consumers’ credit, resulting in significant financial losses, and hurt businesses both directly when their bank accounts are targeted or indirectly when customer information is compromised. These incidences also result in the individual’s tarnished reputation. While those statistics illustrate the growing problem of identity theft in San Diego, it should also be noted that identity theft offenses are grossly underreported (FTC, 2013). This is often attributed to minimal losses and reimbursement by credit card issuers and financial institutions (Allison, Schuck, & Lersch, 2004).
Identity Theft in an Online World

According to Pew Research Center’s Internet & American Life Project, 74% of adults were using the Internet by 2009 (Rainie, 2010). A separate study conducted by Horrigan (2009) during the same time period found that 56% of adult Americans accessed the Internet by wireless means, with the preferred device being a laptop computer. The center also found that from 2006–2008, Internet usage among Latinos rose to 64%, outpacing all other minority groups (Fox, 2009). The significance of those statistics is illustrated by the prevalence of identity theft that occurs using the Internet. A study on identity theft victimization by Copes, Kerley, Huff, & Kane (2010) reported that individuals who regularly utilize the Internet are far more vulnerable to identity theft schemes. Additionally, the most common categories were existing credit card fraud, followed by existing account fraud, and new credit card fraud. This research was consistent with the Bureau of Justice Statistics findings in that credit card fraud far exceeded other types of identity fraud schemes (Langton, 2011).

Identity theft, like other crimes, generally revolves around the three interconnected elements of motive, method, and opportunity (Marshall & Tompsett, 2005). The Internet presents all three elements to aspiring identity thieves. Unsecured networks, malware attacks, phishing schemes, and other gaps in cyber security exploit the lack of authentication available to Internet users and provide opportunities to obtain personal identifying information (Marshall & Tompsett, 2005). A study by Allison, Schuck, and Lersch (2004) focused on the characteristics of victims and offenders as well as clearance rates for law enforcement. That study concluded that identity theft incidents were steadily rising while clearance rates fell. Their findings also cited significant differences between the success of identity theft investigations and other types of property crimes, with the latter experiencing considerably higher clearance rates. The high
volume of victimization among Internet users was driven by the expansion of electronic commerce and online payment methods.

**E-Commerce and Online Payment Systems**

Electronic commerce, or e-commerce, is an industry that unites consumers with retailers and service companies on the Internet. Potential customers can browse products and compare prices from their computers or mobile devices to complete purchases. Transactions occur through secure online payment systems. E-commerce presents several advantages to both consumers and merchants, which was illustrated in 2012 when global e-commerce sales topped $1 trillion, with over 60% of North America accounting for 33.5% of total online purchase (Dusto, 2013). In spite of the criminal activity, e-commerce affords retailers the opportunity to expand beyond their physical regions and access other market shares (Humphrey, Kim, & Vale, 2011). Customers are able to reach merchants or service companies instantly without having to change locations, offering a very efficient experience. While this electronic industry strengthens the economy and supports billions of dollars in tax revenues, it also offers opportunities for identity theft.

Online payment systems deploy a layered approach to security and encryption, protecting transactions from external sources attempting to steal sensitive data. However, one of the most significant challenges in detecting identity theft in online transactions is not protection from data breaches but rather ensuring the legitimacy of the transaction itself. An entity engaging in electronic commerce must authenticate the customer and ensure they have a legal right to the payment medium and associated account being used to complete a purchase. If a retailer authorizes an online transaction only to discover the consumer who initiated the purchase did so without the authorization of the actual cardholder, the merchant will be unable to recover the
losses (Mann, 2011). While several techniques have been deployed to ensure online authentication, including a hierarchal approach to website security certificates and smartcard technology, e-commerce payment systems continue to be targeted by identity thieves (Montague, 2011). The Federal Trade Commission received over 221,000 internet related identity fraud complaints from Californians in 2012, resulting in over half of a billion dollars in losses (FTC, 2013).

For investigators, the most important information captured during online transactions includes e-mail addresses, phone numbers, and shipping addresses. These items are usually unique to the perpetrator and are required for order confirmation (Montague, 2011). Online payments are preferred by identity theft perpetrators since they present significantly less risk to the suspect than in-person transactions.

Online transactions can be completed through different payment methods. The most common are credit card transactions, thanks to the obvious convenience and ability to pay with actual currency at a later point in time (Mann, 2011). Other popular payment methods include bank services such as electronic drafts from checking accounts, payment aggregators such as PayPal, cash alternatives, invoice services, or credit extended by a specific retailer for their products. All of those methods have been exploited at some point by identity thieves to conduct fraudulent transactions (Montague, 2011). Moreover, cross-border commerce in the San Diego–Tijuana region includes online retailing as a convenient and efficient way for U.S. merchants to access the growing market of consumers in Mexico, particularly in populated border areas where Mexican residents consistently embrace American trends (International Community Foundation, 2004). Investigating identity thefts in this border region, like every other major U.S. city, will frequently involve e-commerce transactions.
**Online credit card transactions.** Online credit card transactions are categorized as Card Not Present, or CNP, transactions (Wong, Mirlas, Widong, & Xiaodong, 2003). CNP credit card sales make up a significant volume of the global economy. According to a study by Moody’s Analytics, electronic payments completed with credit cards added $983 billion to the Gross Domestic Product (GDP) of 56 countries examined between 2008 and 2012 (Zandi, Singh, & Irving, 2013). Merchants are unable to physically inspect the cards or compare signatures, placing them at a significant disadvantage (Mann, 2011). A study by Gartner Group, Inc. found that by 2000 credit card fraud with online retailers was 12 times higher than their brick and mortar counterparts (Rosencrance, 2000). A survey of 736 companies by ActivMedia Research, LLC found that websites most susceptible to fraud dealt with online populations that sell merchandise that can be quickly liquidated at high prices such as computers, home electronics equipment, and jewelry (Rosencrance, 2000). A decade later, credit cards were still one of the most common payment methods targeted by identity thieves, with victimization frequently occurring on the internet (Holt & Turner, 2010). Lamberger, Dobovšek, and Slak (2012) reported from their study that microchip technology imbedded in credit cards has decreased card present frauds while increasing card not present schemes, such as online transactions.

**Alternative payment methods.** For the purpose of this discussion, alternative payment methods for e-commerce transactions include non-credit card payments. The most common are bank services, payment aggregators, other cash alternatives, and mobile payments. Bank services include automatic draft payments and debit cards. While identity fraud schemes involving account takeovers usually include cash withdraws or wire transfers, they may also involve online purchases using bank services such as debit cards and automated clearing house (ACH) payments. Debit cards differ from credit cards in that payment is completed through an
electronic funds transfer. Similarly, ACH payments serve as electronic checks (Mann, 2011). However, investigating a fraudulent e-commerce transaction involving a debit card will leverage most of the same information previously identified with online credit card purchases. Investigations of ACH fraud should focus on the bank responsible for the defrauded account (Biegelman, 2009). As of 2011, the FBI estimated that $85 million was lost each year as a result of ACH fraud and unauthorized wire transfers (Apfel & Deichler, 2011).

**Payment aggregators.** Another payment medium that is increasing in popularity is payment aggregators. These are service providers that process payments for e-commerce merchants, with the most popular being PayPal (Montague, 2011). Consumers enjoy the convenience and security of storing their credit card or bank information with one payment system, rather than providing their information to each merchant from which they wish to make a purchase. Merchants enjoy payment aggregators because they can avoid having to set up merchant accounts with a bank or card association (Huang, Zheng, Li, & Kou, 2003). PayPal stores credit card information, accepts currency balances, and even issues debit cards linked to customer accounts (PayPal, 2013). PayPal’s success has made it a prime target for identity thieves.

PayPal is a trusted payment medium among Internet merchants, so perpetrators who successfully create a fraudulent PayPal account increase the probability that a subsequent transaction will be completed and merchandise will ship prior to cancellation. PayPal has also been vulnerable to account takeover schemes, similar to the way bank accounts are targeted (Montague, 2011; Petainen, 2012). However, PayPal has countered the threat of identity theft with the assembly of a robust internal security unit that routinely scrutinizes accounts, encrypts information, and even limits employee access to customer information, creating a more
significant challenge for identity thieves (Huang et al., 2003). Additionally, banks are also offering payment aggregator services to their customers, allowing account holders to setup automatic drafts for all of their monthly bills (McCune, 2005).

**Mobile payment applications.** Mobile payment providers are believed to be the new trend in e-commerce (Birch, 2013). This payment method simply implies an application that can be executed from a mobile device, such as a smartphone or tablet with wireless Internet capability. While this method has yet to gain a significant market share, its popularity is rapidly increasing (Rueter, 2012). PayPal and Visa, for example, have created mobile applications for their customers to make and receive payments (Montague, 2011; Visa, 2013). Financial institutions are also expanding their Internet banking with mobile applications. Mobile payments are considered especially vulnerable to fraud since mobile security is still in its infant development stage (Parnes, Shapiro, Durette, Lee, & Staples, 2013). Identifying whether a mobile device was used to further an identity fraud scheme could assist investigators with identifying the actor through mobile forensic techniques such as device tracking.

Finally, some merchants extend credit directly to their consumers. This method should not be confused with a merchant sponsored credit card, which requires an underlying financial institution and the standard credit card payment system to complete a transaction (Mann, 2011). Credit extended by a specific company can only be used for purchases of their products or related companies. For example, Dell Computers, Inc. maintains a subsidiary called Dell Financial Services, which allows consumers to open a credit account to purchase Dell products (Dun & Bradstreet, 2013). This approach allows the merchant to avoid interchange fees charged by credit card issuers while still allowing customers to make purchases with credit (Mann, 2011). Non-cash payment methods provide opportunities for identity thieves to fraudulently access bank
and credit accounts throughout the U.S. When assessing cross-border identity theft, it is important to understand the trends surrounding contemporary payment systems in Mexico.

**Mexico Embraces Cash Alternatives, E-Commerce, and Internet Banking**

The global reach of electronic commerce has engulfed Mexico’s economy. Mexico’s Internet regulator Asociación de Mexicana de Internet (AMPICI), reported that in 2012 e-commerce purchases in Mexico reached 79.6 billion pesos or $6 billion, a 46% increase from 2011. Most e-commerce related Internet traffic in Mexico occurs in December and November, which combined for 37% of all purchases in 2012. The popularity of e-commerce in Mexico can be attributed to consumers embracing cash alternative payment methods. The AMPICI (2013) reported the most popular online payment methods were credit cards, secured deposit such as money orders, PayPal, and electronic funds transfers.

A separate 2012 study conducted by AMPICI reported that over 37% of Internet users have used some sort of bank product, such as a debit or credit card, for at least seven years. The study also concluded that Internet banking is rapidly expanding in Mexico as more consumers are equipped with the proper technological skills to embrace electronic banking services. Internet accessibility, e-commerce usage, and Internet banking have all contributed to the global rise of identity fraud. The above data suggests that the proper electronic infrastructure exists in Mexico to successfully conduct cross-border identity theft schemes. However, that is not to suggest that Mexicans are suddenly targeting American consumers at alarming rates. Rather, offenders from both the U.S. and Mexico are able to exploit opportunities to complete identity fraud schemes afforded by the Internet while taking advantage of the limitations placed upon law enforcement by the international border.
Cybercrime and Identity Theft in Mexico

The AMPICI (2013a) estimates the presence of over 40 million Internet users in Mexico, a country that has become increasingly wireless and technologically advanced during the last decade. While Mexico’s economy has grown substantially through international trade and e-commerce, dishonest Internet users have emerged as well. As a result, Mexico has become the cybercrime and identity theft capital of South America (Tatone, 2013). Similarly to the United States, hackers target databases containing personal identifying information as well as individual consumers through scams such as e-mail phishing (Tatone, 2013). Identity theft and data breaches became such a widespread problem in Mexico that it prompted the creation of Mexico’s consumer-protection agency, Procuraduría Federal del Consumidor, or Profeco. Profeco is required to answer Internet complaints within 15 days, although enforcement of consumer protection laws in Mexico is weak (E-commerce, 2008).

According to a recent survey completed by Norton, an international cyber security firm, cybercrime and data breaches cost Mexico $3 billion per year (Southwick, 2013). A 2007 report on Mexico’s cyber infrastructure identified Baja California, the state in which the city of Tijuana is situated, as having the second highest concentration of households with computers and Internet users (Anonymous, 2007). This is partially the result of the influence from neighboring San Diego, a city that provides access to modern technology and wireless capabilities. The data from the research demonstrated that opportunities to commit cybercrime and online fraud, which include identity theft, continue to grow in Mexico particularly along the border with California.
Geopolitics and Cross-Border Travel

The city of San Diego boasts an estimated population of 1.3 million residents (San Diego Association of Governments, 2013). Tijuana is Mexico’s fifth largest city and is situated along the border just south of San Diego, with an estimated population of 1.6 million residents (United Nations, 2010). San Diego’s border region coincides with an area referred to as South Bay, which encompasses the cities of National City, Chula Vista, and Imperial Beach, along with the city of San Diego neighborhoods geographically located between Chula Vista and the U.S.-Mexico border. The total estimated population of this region based on data collected by the San Diego Association of Governments (2013) is around 430,000 residents. One of the most unique geographical characteristics of San Diego is its proximity to Tijuana. The two cities combined make up the largest transnational metropolitan area in the world (International Community Foundation, 2004). The two official border crossings that connect the cities are the San Ysidro Port of Entry, which is the busiest international border crossing in the world, and the Otay Mesa Port of Entry, which is settled in the far southeastern border area of San Diego and serves as the region’s largest commercial border crossing (U.S. Department of Transportation, 2013).

In 2012, a total of 27.7 million individual border crossings occurred from Tijuana into the city of San Diego through the San Ysidro Port of Entry, which included over 6 million vehicles (U.S. Department of Transportation, 2013). Tijuana residents regularly cross into San Diego to enjoy a plethora of shopping, recreational, educational, or business opportunities. Likewise, San Diegans frequent Tijuana to access inexpensive medical services, purchase cheaper retail goods, enjoy the historical entertainment district, or visit emerging restaurants (Urban Land Institute, 2013). Both cities promote tourism and amenities to boost their local economies. Both economies are deeply integrated with transportation services and production chains routinely
crossing the border in both directions. Consequently, both local governments regularly facilitate communication to improve working relationships and connected infrastructures.

**San Diego and Tijuana: Interconnected Economies**

Mexico is the recipient of 31% of San Diego’s exports and 642,000 jobs in California are directly related to trade with Mexico (Wilson, 2011). Major manufacturers use production sites on both sides of the border to create goods and manage supply chains. It is not uncommon for products to crisscross the U.S.–Mexico border several times before completion (Wilson, 2011). The interconnected commerce results in a workforce and social networks that straddle the border. Thus, large populations of Tijuana residents enter the United States on a daily basis to work labor-intensive jobs, transport goods from Mexico into the United States, or visit family members that live and work in the United States. Employment in San Diego’s border region is fueled by financial and retail services, including various stores, currency exchanges, pawn shops, restaurants, and banks. With so much routine cross-border commerce, identity theft opportunities frequently present themselves as Mexican residents employed in the U.S. are granted access to information and technology that were previously unavailable in their native city. Also, those who routinely cross the border into San Diego for illegitimate purposes are able to do so under the guise of a member of the ordinary traveling public. U.S. law enforcement efforts can be complicated when cases involve suspects or even victims from Mexico.

**Cross-Border Fraud: A Growing Concern for U.S. Border Regions**

Cross-border fraud is a recognized issue for both the United States and Mexico. Profeco signed a bilateral agreement with the United States government in 2005 to ensure cooperation in the fight against cross-border fraud (Profeco, 2012). While the agreement is not legally binding, it established the commitment to improve cross-border coordination with anti-fraud efforts.
According to a 2008 study by KPMG, 77% of companies in Mexico were the victim of at least one fraud incident during the previous year (Segura, 2009). Similarly to the United States, Mexico experienced an economic depression that increased unemployment, particularly in urban areas like Tijuana. Many fear that such widespread hardship will only increase the incentive to commit fraud (Segura, 2009).

In the United States, most corporations with both a domestic and international presence lack the proper procedures to investigate cross-border fraud (Oswalt, 2007). A KPMG survey of corporate executives resulted in widespread opinion that cross-border fraud will only get worse and over 56% reported a lack of investigative protocols within their companies for cross-border investigations (Oswalt, 2007). The Organization for Economic Cooperation and Development (OECD) recommended that member countries, including Mexico, develop best practices for cross-border fraud investigations, to include identifying and overcoming barriers (“Usage of payment cards,” 2011). The broader context of transnational fraud has become widely recognized, as the internet has made international boundaries irrelevant for identity fraud perpetrators (Barker, D’Amato, & Sheridon, 2008). More specifically, identity theft is a global issue that cannot be ignored, particularly between such interconnected economies as the United States and Mexico. Border regions such as San Diego that exercise a significant amount of cross-border commerce are especially vulnerable to cross-border fraud.

Understanding Border Security and Crossing Data

Maintaining the flow of information from both sides of the border is significant when attempting to locate, track, or apprehend suspects that operate on both sides of the U.S–Mexico border. U.S. Customs and Border Protection (CBP), is tasked with securing the U.S. border entry points and has the unique authority to search and investigate anyone who enters the United States
Federal statutes authorize CBP to search, “All persons, baggage and merchandise arriving in the Customs territory of the United States,” which includes electronic devices that store information such as computers, mobile phones, and external storage devices (CBP, 2010, p.1). CBP Officers verify the identities of travelers who hold non-U.S. passports or visas through the U.S.–VISIT program, using electronic fingerprint and photograph technologies maintained by the Office of Biometric Identity Management (CPB, 2013a).

Data that can assist with cross-border investigations is maintained at official border crossings. Biometric information obtained from the U.S. –VISIT program is stored in Department of Homeland Security repositories. Non-Mexican citizens, visitors who plan to stay longer than 30 days, or visitors planning to travel outside the border zone must complete an I-94 arrival/departure form. The I-94 form includes basic information including name, birthday, home address, temporary address in the United States, date issued, city where the visa was obtained, and passport number (Westphal, 2009). Some visitors complete the I-192 form, or application to visit the United States as a nonimmigrant. That form collects the same information as the I-94, including detailed reason for the subject’s visit (CBP, 2013a). Upon entry, the visitor must complete the U.S.–VISIT procedure where their digital fingerprints and photograph are recorded. If it is discovered that false information is provided on either form, the individual could be removed and denied future entry into the United States.

Finally, the U.S. Department of Homeland Security established the Secure Electronic Network for Travelers Rapid Inspection program (SENTRI). This program issues an electronic card called a SENTRI pass for expedited inspection when utilizing a land crossing from Mexico into the United States. In order to obtain a SENTRI pass, individuals provide all of their personal information and undergo biometric confirmation and a thorough background check (CBP,
Although SENTRI-approved travelers are considered low risk, the information maintained about them could be helpful should one become the target of an investigation. All of the above data collected by CBP is stored by U.S. Citizenship and Immigration Services and made available to law enforcement personnel, providing potential sources of intelligence in cross-border investigations (Westphal, 2009).

**Law Enforcement Challenges with Identity Theft Investigations**

Globalization and the expansion of Internet applications have provided an opportunistic environment for identity theft perpetrators and a very challenging one for law enforcement. Identity theft offenses are frequently committed by persons outside of the jurisdiction in which the victim resides, and in some cases outside of the country (Finklea, 2012). Cyber investigation capabilities are vital when attempting to investigate an identity fraud scheme that utilizes the Internet in some capacity, from dissecting fraudulent online transactions to infiltrating Internet forums that trade stolen credit card information. A law enforcement study by Gogolin and Jones (2010) found that participating agencies were not prepared to successfully conduct digital investigations. Most cited a lack of training and resources and only half of the surveyed agencies reported having at least one officer trained in collecting and storing digital evidence, even though over 90% of the participating agencies investigated identity theft offenses. That study suggested most law enforcement entities, particularly at the state and local levels, embrace traditional investigative methods that do not require a high degree of technical knowledge. A lack of cyber investigative knowledge, skills, and abilities not only inhibits an agency’s capability to counter high technology identity frauds, but also limits its resources in unraveling identity fraud networks and organizations (Gogolin & Jones, 2010).
Conducting effective investigations of large identity fraud networks requires methodical and tedious analysis. Organized identity theft rings frequently apply layers, protecting the leaders by deploying “front men” to steal PII or accept items received at shipping addresses (Collins, 2006). These low-level individuals may retrieve items that were purchased using the victim’s credit cards or retrieve payment cards from new accounts opened with the victim’s information from mail box service stations. Similar to narcotics distribution networks, law enforcement frequently encounters the lower level operators, failing to dismantle the broader network of criminals that cause the most harm to consumers. A study by Campana and Varese (2012) concluded that effective use of telephone wire-taps coupled with comprehensive data analysis provides unprecedented insight into criminal networks. Criminal networks have the capability of inflicting harm on numerous victims; therefore, law enforcement should be equipped for an effective response.

**Identity Theft Networks**

An alarming trend is the presence of identity theft networks, where numerous individuals collude to execute large-scale identity frauds with a high volume of victims. These networks may include organized crime groups, such as transnational gangs, or relatives working together to obtain illicit funds (Newman & McNally, 2005; Collins, 2006). A comprehensive study by ID Analytics identified 10,000 identity fraud rings in the United States. Although most fraud rings were concentrated in the Southeastern United States, the southwest region, including Southern California, also experienced organized identity fraud groups. Some networks target friends and family members while others victimize complete strangers (Coggeshall, 2012). The Identity Theft Resource Center predicted that organized crime groups will become increasingly involved in identity theft schemes, particularly credit card fraud, and these crimes will be largely
transnational (Finklea, 2012). Research also indicated that most local law enforcement agencies are not properly equipped to investigate such complex networks and schemes (Newman & McNally, 2005).

**Analyzing Data Findings from the Literature Review**

This project began with a review of the literature on identity theft, cross-border fraud, and related factors in Mexico such as the rapid expansion of e-commerce and Internet access. The literature review presented research findings from previous studies on identity theft victimization and law enforcement response. Those results suggest that most identity thefts involve the Internet in some fashion, either to acquire the victim’s information, to use it, or both. Even though many of San Diego’s identity theft perpetrators are unsophisticated methamphetamine addicts, the typical schemes involve simplistic methods of acquisition of a victim’s PII through larceny or dumpster diving followed by an Internet-driven point of use, such as completing fraudulent online purchases with stolen credit card information or electronically applying for a new credit card account (Biegelman, 2009). The study by Gogolin and Jones (2010) found a lack of cyber investigative capabilities within law enforcement agencies to respond to technology-driven identity theft schemes. While that study focused on the state of Michigan, it echoes a nationwide trend where traditional policing tactics still dominate academy training curriculums. The rapid expansion of Internet use, e-commerce, and payment cards in Mexico, particularly in the state of Baja California where Tijuana is situated, also suggests that cross-border identity thefts are electronic in nature, which parallels the trends throughout the U.S. and the rest of the world (Matthews, 2013).

Most identity theft-related research focuses on prevention and detection, followed by victimization. The literature significantly lacks methods to investigate an identity theft case from
the moment a police report is taken to indicting a suspect for prosecution. The goal of this project was to identify the most cutting-edge investigative methodologies to assemble a framework in response to cross-border identity thefts in the San Diego–Tijuana region, using tools and techniques designed to connect the point of use of a victim’s personal identifying information with an actual perpetrator. The review of research studies, surveys, and personal accounts by practitioners suggests that most identity thefts involve the Internet, where suspects are able to execute schemes without being in the presence of merchants poised to contact law enforcement the moment a transaction is flagged or witnesses prepared to provide their description to investigators. Additionally, there is clearly a gap in digital forensic capabilities among law enforcement entities. As a result, this study focused heavily on best practices for conducting investigations of identity thefts involving the Internet and mobile devices.

Many law enforcement units tasked with investigating identity thefts are grossly understaffed and underfunded. This typically drives a triage approach to cases, where those that involve in-person transactions with an identifiable suspect are readily investigated while electronic schemes, particularly cases with a nexus to Mexico, are deemed unsolvable and not investigated at all, reiterating the need for an investigative framework for cross-border investigations with digital forensic techniques.

**Research Methods**

The research for this project was completed through keyword searches in academic databases and by reviewing books authored by industry experts and practitioners. The literature review identified the main challenges presented in investigating cross-border identity thefts which include the use of the Internet to complete schemes, and a lack of available suspect information during preliminary investigations. Researching solutions included an analysis of
cyber investigative techniques that were developed in response to other types of technology-based crimes, such as network intrusions and distributed denial of service attacks. Those types of investigations rely heavily on cyber forensics to trace the location of a suspect, and thus could assist in resolving an identity theft scheme where the suspect’s location is unknown. Tactics that are currently employed in various types of investigations, such as forensic analysis of mobile phone devices, were researched and applied as well. As information was gathered to formulate investigative methodologies, it was applied to hypothetical cross-border identity theft cases. That approach assisted in ascertaining additional challenges that needed to be addressed to create an effective framework within which an investigative strategy could be created in response to cross-border identity thefts in the San Diego–Tijuana region.

**Research Findings**

**Identifying Preliminary Investigative Leads**

The research into investigative methods began with the fundamentals of e-commerce and online payment applications in order to identify information gathered during a preliminary investigation, which typically form the first leads. When an identity theft suspect places an online order with a victim’s credit card or opens a new bank or credit account using a victim’s PII, information is captured that is readily available for forensic analysis once an investigation commences. This includes an Internet Protocol (IP) address that references the location from which a suspect connected to the Internet. The IP address is read by the server through the data packet, which simply refers to the method in which information is transmitted from one network to another. Additionally, online merchants and financial institutions require verifiable attributes such as phone number, e-mail address, and a physical mailing address.
The above attributes are part of the authentication process, such as mailing an inactive credit card and then requiring the new cardholder to call a designated number for activation or clicking on a link in an e-mail. If a merchant or card issuer sends a confirmation e-mail only to receive a return message stating the e-mail address was invalid, the order may be canceled. As a result, suspects will usually provide information they actually have access to, such as their own mobile phone number and e-mail address, to ensure a successful transaction when using a victim’s PII. While that information may only be used for the particular scheme and then discarded by the suspect, the captured details still have value for a post mortem forensic examination.

A mailing address that the suspect has access to is required to take possession of ordered products or new credit cards that require activation. Even account takeovers, which are digital in nature, typically involve a physical location at some point to take custody of the stolen currency through cash withdrawals or debit transactions. Providing falsified information or simply using the victim’s e-mail and phone number could prevent verification and result in an unsuccessful scheme. California Penal Code §530.8 (2006) requires disclosure of transaction information to investigators designated by the victim.

**Investigative Techniques for Location Tracing**

The above findings guided further research into leveraging the captured information to locate the suspect responsible for using the victim’s PII. That research focused on forensic techniques that trace the source of IP addresses, data packets, and e-mails. Also, cell phone forensics were introduced, with research findings that include capabilities to locate a mobile device at a particular day and time, assisting with the goal of identifying the suspect’s location at the point of use stage of the identity theft scheme. Once located, Wi-Fi surveillance was
identified as one of the best techniques to observe a targeted individual and determine any additional identity frauds they may be conducting.

**Data Analysis: The Big Picture**

During the course of the research, a major challenge that needed to be addressed was managing data collected during complex investigations, linking similar cases, and maximizing the value of arrests. The literature review provided statistics that included thousands of identity theft complaints received in San Diego County during 2012. With limited investigators, data analysis provides an effective method to identify trends and patterns among cases, changing the way they are viewed by those assigned to solve them. For example, several cases that report losses of small dollar amounts may appear insignificant by themselves; however, if those cases are connected to one suspect or group they combine to create one large investigation of a serial offender(s). Data analysis provides the best opportunities to illustrate the big picture among datasets.

Finally, social network analysis was researched as the preferred method of maximizing the value each arrest by determining whether one individual is operating within a broader criminal network. By doing so, additional targets can be identified to expand the investigation. For this project, link diagrams were the recommended method of data and social network analysis, allowing for quick reference and interpretation. These findings assembled the framework to guide law enforcement at all levels through investigations of cross-border identity thefts in the San Diego–Tijuana region and are described in detail throughout the sections that follow.
Exploring the Digital Footprint

Understanding Internet Protocol Addresses

When an individual connects to the Internet, they actually connect to their Internet Service Provider (ISP), which provides web connection services for a fee. Currently, most consumers use broadband networks with wireless capability for faster connection speeds (Smith, 2013). When an ISP provides the connection, it assigns the user an identifier known as an Internet Protocol (IP) address. This IP address is assigned to either a specific user who is hardwired to the Internet through an Ethernet cable, or to a router that provides a wireless connection to anyone who can successfully access it (Anderson & Benedetti 2009). ISPs utilize IP addresses to maintain billing records and track usage (Reyes et al., 2007). Therefore, IP addresses are assigned to a specific person or company. There are two types of methods for assigning IP addresses: statistical or dynamic.

A computer system uses a network interface card (NIC) to connect to a typical type of network, media, or protocol. A statistical assignment of IP addresses simply involves configuring the computer’s NIC with a specific IP address during installation (Whitman & Mattord, 2012). Each time a connection is made through the ISP, the IP address will identify that specific connection location. A significant disadvantage exists with assigning static IP addresses in that the pool of potential customers serviced by the ISP becomes limited. The business solution to that limitation is dynamic IP address assignment. This method does not specifically assign an IP address to one connection port. Rather, during installation a computer’s NIC is set up to obtain an IP address assignment through its designated server each time it connects to the Internet (Reyes et al., 2007). Using dynamic IP addressing, the ISP maintains its predetermined number of IP addresses and simply assigns them as needed. The ISP is relying on the likelihood that not
all of its users will connect to the Internet at the same time, and therefore can maintain more
users than IP addresses since the IP addresses are unassigned and used as needed. It is important
to note that a computer could use multiple IP addresses in one day or even in the same session,
particularly if connection is interrupted and the computer must reconnect (Whitman & Mattord,
2012). Investigators must understand the difference between the two methods of IP address
assignment. The statistical method references a static connection site whereas the more common
dynamic method depends entirely on the date and time stamp to determine the specific user.

**Tracing IP Addresses**

When information is sent over the Internet, it transmits as an encoded signal for faster
connection speed and conservation of memory space (Anderson & Benedetti, 2009). Once
received by the destination computer, it is converted into binary code, which is a computer
programming language, then decoded to appear in a readable format. That data is transmitted in a
package referred to as a data packet. Webservers such as online retailers, e-mail servers, and
electronic banking applications capture IP addresses from the data packets transmitted by the
consumers accessing their websites.

The actual data within the packet is called a payload and is preceded by a header or
protocol frame, which organizes network traffic so the receiving device knows how to read the
information it contains (Anderson & Benedetti, 2009). The header includes the originating and
destination information and an Internet protocol (IP) header. When sent over a network, the
header would also include the media access control (MAC) address of the device that created the
packet (Anderson & Benedetti, 2009). Each data packet includes an IP header, which is the
information that precedes the data (Flor & Guillory, 2011). The header contains important
information about the data, and serves as the communication and control link between the
protocol elements of the different devices (Ponec, Giura, Wein, & Brönnimann, 2010). Most importantly, the packet header includes information that identifies the source of the message, including the IP address.

IP addresses can be traced through the ISPs, which maintain detailed records of clients who connect to the Internet through their service (Reyes et al., 2007). During an investigation, any IP addresses captured should be requested. Once an IP address is identified, it can be queried in the Association of Registered Internet Numbers, or ARIN. The results display the ISP to which the queried IP address is assigned, along with a point of contact. Investigators will need to complete a search warrant of the ISP to obtain the user information associated with the IP address during the time period specified. When IP headers from data packets are obtained, they may include markings from the routers through which the data packet passed as it moved from the sender to the recipient (Aljifri, Smets, & Pons, 2003). IP addresses can be traced through data packet analysis, which will be discussed later. IP addresses are the first step in tracing online activity, since they only identify the connection port that allowed a specific node to connect to the Internet.

**Connection ports.** The most common connection ports are wireless routers and Ethernet cards. An Ethernet card allows a hardwired computer to connect to the Internet through a local area network (LAN) cable. Thus, hardwired computers are easier to associate with an IP address than a wireless connection. Wireless Internet connections are made through routers, which are devices used to connect an internal network to the external Internet, or simply facilitate a connection to the ISP for Internet access (Whitman & Mattord, 2012). Routers are an important component to cyber investigations since they are also assigned MAC addresses and can be located through their assigned network name, such as a generic “Netgear” or a name conducive
to the administrator, such as “John Doe’s Wireless Network.” The most important factor regarding routers is that they can be configured to store valuable information for an investigation.

Routers may store traces from data packets that pass through them, identifying the source of transmissions that accessed the network (Aljifri, Smets, & Pons, 2003). This configuration is less common on small localized networks since it affects the speed and performance of the router. Administrative logs that track which devices accessed the router are more common. This capability involves storing MAC addresses from devices that are authorized to access the network and the Internet activities associated with them (Anderson & Benedetti, 2009). IP addresses can be traced to a connection port, at which point an investigator must identify the specific device that accessed the router and the individual who owns it.

**Identifying specific devices.** Identifiers for specific hardware devices include hostnames and MAC addresses. Hostnames are assigned to specific devices on a network and are usually established using the location of the device or program name. For example, a hostname in a police department, “HQ_Robbery1” would likely identify hardware located within the Robbery Unit at Police Headquarters, such as a computer workstation or printer. MAC addresses are often referred to as electronic serial numbers or hardware addresses. They are difficult to change since they are usually burned into the ROM chip on the computer’s Network Interface Card (NIC) by the manufacturer and can also be used to track connectivity (Whitman & Mattord, 2012). If an investigator is able to determine the MAC address of a device, then the specific network interface card used for Internet connectivity with that device could be identified. Once the computer that contains the identified NIC is obtained, a forensic analysis could uncover software and peripheral devices used, even after disposal, with the system (Moore, 2011). However,
hostnames and MAC addresses could be changed or disguised through a process called MAC spoofing, which is usually accomplished with certain hardware or software combinations (Reyes et al., 2007).

In order to view a computer’s MAC address on a Windows machine, begin with the command line prompt screen. This is found under the start menu under accessories or by selecting “Run” and typing “cmd.” On a Macintosh, start at “System Preferences” and in the search entry box type “Ethernet ID” and press the return button on the key board (Reyes et al., 2007). While this is a simple step, it is an important one since the investigator is seeking a match between the computer and the MAC address found on a router log. When MAC address spoofing is suspected, a more in-depth forensic analysis of the computer would reveal the actual serial number and the file that accomplished the spoofing during the data transmission (Moore, 2011).

**Limitations of IP Address Tracing**

While successful traces of IP addresses could ultimately lead investigators to a suspect committing identity fraud through the Internet, there are limitations to this approach. Any device equipped with wireless capability within a router’s range can potentially utilize its connection to the Internet. Therefore, if multiple devices and users connect to the Internet using the same router, they will also register the same IP address (Reyes et al., 2007). Wireless networks could be accessed without authorization, leading the recipient of the Internet traffic to believe it originated in one network when in fact the user is unknown. Some of the most effective methods of disguising an IP address include the use of web proxies and anonymizers.

**Challenges of web proxies and anonymity applications.** A study by Edman & Yener (2009) found that web proxies, commercial anonymity applications, and the Tor web browser are the most commonly used Internet tools to hide a user’s IP address. Web proxies are centralized
servers that a user can connect through when communicating with a desired website. As a result, the website captures the IP address of the proxy rather than the actual user. Proxy servers are one of the most common methods of masking an IP address since they are easily accessible by Internet users (Edman & Yener, 2009). When operating with a proxy, the proxy server will relay the user’s request to the destination followed by the response back to the user, removing the user’s IP address to provide basic anonymity. However, while the destination is unaware of the user’s IP address, the proxy server has access to both the source and the destination and therefore is equipped to trace user activities (Li et al., 2013). Also, proxy servers tend to have the weakest security against observers (Edman & Yener, 2009). Monitoring incoming and outgoing traffic can provide a high level of information about the users attempting to disguise themselves. Web users who wish to remain anonymous frequently use proxies that are based overseas. In such instances, a traced IP address would indicate the source of the activity resides in a foreign country, deterring investigators from conducting further inquiries.

![Figure 1. Basic web proxy model. This figure illustrates how a web proxy anonymizes the source of data transmitted over the internet.](image)

Commercial services also provide basic anonymity, such as Anonymizer.com and GoTrusted.com. For these systems, clients must pay a subscription fee in order to utilize the servers to mask their IP addresses. However, since these companies are in charge of all communications that pass through their servers, they are able to record such relays and thus they do not provide total anonymity (Li et al., 2013). A search warrant would require the company to
surrender specific subscriber information. With deferred notification, the information would be obtained unbeknownst to the client.

**Tor browser: Roadblock to traceability.** One of the most popular anonymous web applications is the Tor browser, which allows users to conduct Internet activity with complete anonymity. Tor is a low-latency overlay network that deploys TLS encryption of its communications, preventing webhosts from identifying the IP address or system information of their clients (Li et al., 2013). The Tor browser uses an onion routing system, which is considered the most prevalent system design for anonymity. Onion routers deploy a complex communication approach where data transmits through a network of servers, where each server only receives a piece of the data packet before it is reassembled as it passes through the browser’s exit node (Li et al., 2013). As a result, the transmission is untraceable. Some experts have theorized that since the entry guard and exit nodes of the Tor browser contain the source and destination of the anonymized communication, it can be decoded to reveal tracing details (Li et al., 2013). However, this concept has yet to be successfully demonstrated.

Before an investigator could begin to unravel an IP address masked by a proxy or Internet anonymity application, he would first need to determine if the captured IP address belongs to a proxy in the first place. In most cases, even a proxy or anonymous browsing application includes some originating information in the packet header (Li et al., 2013). Master lists of IP addresses used by proxies are easily obtainable via the Internet, or can simply be verified by querying the IP address through ARIN. Once the use of a proxy is established, an investigator should begin targeting the server or company to obtain the user’s actual information. Once again, the date and time stamp is critical to pinpoint which client sent the request through the proxy server. Experienced identity thieves who operate through the Internet often ensure that the IP addresses
captured by merchant servers are spoofed or entirely falsified. In such cases, forensic analysis of the data packet headers and payloads could assist with successful tracing.

**Tracing Online Activity Through Forensic Data Packet Analysis**

When the suspect’s IP address is disguised or hidden from the recipient altogether, data packet tracing techniques can be deployed to overcome this obstacle. While the most sophisticated cybercriminals create layers of anonymity that prevent source identification, many identity thieves do not possess that level of dexterity. When an investigator traces the disguised IP address, the result will either identify an anonymity service or proxy, or simply read that the address is untraceable. A possible solution to this involves data packet tracing, which is a computer forensic technique originally developed in response to denial of service attacks on networks (Aljifri, Smets, & Pons, 2003). Different approaches to forensic data packet analysis have been deployed during cyber investigations. The research for this project yielded two techniques that appeared to be the most useful for this framework. The first involves payload attribute analysis to digitally fingerprint the data for comparison, and the second utilizes packet header compression and analyzing packet markings to reconstruct the electronic path traversed by the data packet.

Payload attribute systems provide a unique opportunity to complete a forensic examination of the data packet header and payload to complete a backwards trace from the destination to the source, particularly in less sophisticated schemes. Most anonymizer protocols could hide the header or strip the packet of its header altogether (Prasad, Reddy, & Jyothsna, 2012). However, a forensic analysis of the data itself could still identify unique payload attributes that serve as a form of a digital fingerprint, assisting investigators in tracing its origin. This process, which serves as a form of digital fingerprinting, converts payloads and headers into
a unique hash string that could be compared to other Internet traffic with very few false positives (Sembiring, Istiyanto, Winarko, & Ashari, 2013).

**Digital Fingerprinting**

Hash functions are an encryption technique that utilizes mathematical algorithms to convert files into a fixed length digest, which is sometimes referred to as a digital fingerprint since it is unique to a particular payload (Schleimer, Wilkerson, & Aiken, 2005). Comparing digital fingerprints assists web browsers and servers in determining whether a remotely transmitted file was modified or poses a threat to the network. Hash files confirm the identity of a message and any changes to its content. Message identity and integrity are critical for e-commerce applications (Whitman & Mattord, 2009). Hash functions are frequently used in password verification systems to confirm the identity of the user. The hash file of the original password is calculated and stored for later comparison. Each time the user logs on with that password, the system calculates a hash value based upon the input and compares to the stored digest in order to confirm identity (Whitman & Mattord, 2009). Using digital fingerprint comparison is a concept that could be applied to the cyber forensic portion of an identity fraud investigation. A contemporary version of digital fingerprinting uses the Winnowing Multi-Hashing (WMH) approach for payloads for file storage and comparison with fewer false positives than the more commonly used hash algorithms (Aljifri, Smets, & Pons, 2003).

**Digital fingerprinting through WMH.** The WMH technique uses an algorithm procedure that converts a large data item, such as a payload or file, into a shorter, yet unique hash file that identifies the payload (Ponec et al., 2010). First, the file undergoes a payload attribution procedure to identify unique data strings for later comparison (Sembiring et al., 2013). Rabin Fingerprinting, a method developed my Michael Rabin, utilizes a digital fingerprinting
scheme based on polynomials, using short checksums of hash strings within the data property to identify unique attributes (Ponec et al., 2010). Winnowing is believed to be more accurate than Rabin Fingerprinting, because it utilizes an efficient algorithm that enables accurate detection of full and partial copies of data strings between documents (Ponec et al., 2013). The WMH procedure combines Rabin Fingerprinting and Winnowing, reducing the probability of false positives during comparisons.

Winnowing Multi-Hashing was developed as a hash-based tracing technique for payloads and IP headers (Sembiring et al., 2013). WMH converts the data into a hash file and then breaks it up into blocks, which are then stored in a Bloom filter available for query when the comparison occurs (Ponec et al., 2010). An investigator does not need to possess the skills to manually apply the WMH method. As with other forms of hash functions, user-friendly software would complete the WMH conversion process. Once the file is converted, the new value is stored for comparison with other WMH files to find a match. For example, if an investigator obtains the data packets from an e-commerce webserver that were sent by a suspect, those files would be converted using the WMH process and then compared to files retrieved from the suspect’s local network. This technique is similar to comparing the fingerprints found at a crime scene to a potential suspect.

**Identifying the Source of a Data Packet Using WMH Values**

The first step in tracing the data packet to its origin is identifying the time interval that it appeared on a network or server. Time intervals are used since the precision of date and time stamps usually lack 100% accuracy, particularly when data passes through several servers as it moves closer to its destination (Pang, Allman, Paxson, & Lee, 2006). Once the time interval is identified, the payload attributes are converted to a digital fingerprint using the WMH method.
The fingerprinted packet becomes the control packet, since it has been assigned a unique identifier to compare to other packets. Domain keys and other unique attributes could be extracted to provide bits of information regarding which servers a packet was routed through (Leiba & Fenton, 2007). As those servers are investigated, stored packets can be data mined to identify a match. Converting files to WMH also preserves privacy, since the actual data is not being viewed, but rather its converted bit string.

Recall that the initial communication with most proxies and anonymity applications, including the Tor browser, is not encrypted and thus the actual IP address of the user can usually be identified. Through data mining, the data packets that entered the anonymity application during the preselected time interval can be analyzed and fingerprinted with the WMH method. The investigator simply needs to compare the WMH attributes of the incoming packets to find a match with the control packet. Once a match is discovered, the IP address of the packet entering the anonymity application can be extracted and successfully traced, since theoretically the IP header has yet to be disguised. That packet should still contain its payload header with the source’s originating information, including the user’s IP address and specific connection port, leading the investigator to the origin of the transmission (Anderson & Benedetti, 2009). The header may also include the MAC address of the packet source. If not, the logs from the router or connection port can be analyzed to determine which MAC address utilized the IP address in question in conjunction with the date and time stamp. Figure 2 below illustrates the basic theory behind WMH comparison.
Data Packet Tracing Through PPM and Header Compression

Methods of forensic data packet analysis that focus on actual tracing are Probabilistic Packet Marking (PPM) and compressed edge fragment sampling. The drawback to these methods is they are dependent upon router configuration; however, they can prove extremely effective. PPM aims to ensure that the path of a data packet cannot be falsified when it travels between the suspect’s PC and the target. This approach establishes an audit trail by adding bits of tracing information to the packet as it passes through each router (Aljifri, Smets, & Pons, 2003). The routers must be configured with packet marking schemes that interlink the router’s IP address in the packet header (Aljifri, Smets, & Pons, 2003). A major limitation with this strategy is that packet headers lack the storage space to maintain the additional information. However, that challenge is overcome by compressed edge fragment sampling, which uses the IP fragment
identification field within the IP header to store compressed bits of tracing information within the data packet header (Savage, Wetherall, Karlin, & Anderson, 2001). Cisco routers, which control around 85% of the global router market, are manufactured with implemented packet marking schemes (Aljifri, Smets, & Pons, 2003). Many networks already include this feature as a cybersecurity protocol to thwart or respond to cyber-attacks. Investigators should be aware of this concept and inquire into router capabilities of entities that were unwillingly involved in identity theft schemes.

**Considerations with Virtual Private Networks**

With Virtual Private Networks (VPNs), IP packets are usually sent in transport mode or tunnel mode. In transport mode, the payload is encrypted but the packet header is not, allowing a third party to view the source and destination (Whitman & Mattord, 2012). In tunnel mode, the entire packet, header included, is encrypted until it reaches its destination, in which case the recipient uses a decryption key to read the packet. When tunnel mode is used, the most efficient packet inspection approach requires retrieving the decrypted version from the intended recipient. The WMH approach to digital fingerprinting takes encrypted payloads into consideration, but the encryption could affect comparison with the non-encrypted version of the packet. Retrieving both versions of the packet would be ideal before attempting to trace to their path.

**Application of Forensic Data Packet Analysis**

Several entities have robust cyber security systems in place that are designed to capture and analyze data packets and monitor system log files for servers and routers. These configurations are implemented in response to a growing number of cyber-attacks and costly network intrusions. While data packet analysis and tracing techniques have mostly been limited to use in hacking incident investigations, the available information can be utilized for other types
of investigations as well. Once a data packet lands on a server, the entity owns it. If it is still archived, an investigator should use this valuable piece of information for tracing the identity theft suspect’s Internet connection location. If the method of acquisition of the victim’s PII involved a network breach or phishing e-mail, then a successful cyber investigation that includes a data packet trace paralleling the investigation into the point of use of the PII could piece together the entire scheme and ultimately identify most, if not all, of the individuals involved. As identity thefts become increasingly digitalized with the availability of an online environment, investigative techniques should also correspond with appropriate computer forensic capabilities.

Computer forensic software plays a significant role with the implementation of data packet tracing. Forensic software is capable of rapidly identifying and sorting headers, digitally fingerprinting the payload, and even completing the tracing process. Programs such as EnCase should be utilized to maintain the chronology of information obtained, such as WMH values along with MAC and IP addresses, for comparison to a suspect’s computer once it is located and examined. Continuing developments in forensic software allows field investigators to become trained in these computer forensic techniques without acquiring a lengthy background in computer science.

**Limitations of Tracing Data Packets**

While digital fingerprinting and extracting PPM markings from packet headers can be used to conduct successful traces, there are limitations. The destination server maintained by the entity as well as the external router or port that grants access to the secured network should record the data packet and its attributes. In some cases, the information is not stored for very long and may be unavailable by the time a crime is discovered and an investigation is underway. Retrieving the data packet requires the assistance of in-house IT personnel or access granted to a
Some entities do not wish to devote the time and resources to assist law enforcement inquiries, particularly if the loss is below a certain threshold. Additionally, law enforcement entities may not agree with the cost benefit analysis of the required software and personnel for data packet tracing, especially since it is a new concept for most organizations.

Certain anonymizers such as Tor use complicated onion routing networks, making it nearly impossible to identify the specific point where the unencrypted data packet entered the browser (Li et al., 2013). Similar to IP addresses, certain data packets simply cannot be traced entirely to the source. Meta searches on the web could identify points in which a suspect inadvertently discloses identifying information in blogs or social media websites, which was the type of mistake that brought down one of the most sophisticated anonymous cybercrime networks in U.S. history (Olson, 2013). If a data packet is determined to be untraceable, its attributes should still be stored in the event the user’s computer is located and seized. A successful trace would need to rely on other mistakes made by the suspect, such as sending traceable e-mails or disclosing a mobile phone number.

**Forensic Examination of E-Mail Messages**

When e-mail messages sent by a suspect are recovered during an identity theft investigation, valuable information can be extracted to identify the location from which they were sent. When an e-mail travels from the sender to the recipient, it passes through several servers, leaving a digital path that connects the two parties. While the perpetrator could easily open a new e-mail account used solely for the scheme, even a single e-mail sent to confirm an online order or new account application using a victim’s information could potentially reveal the perpetrator’s IP address. In order to properly extract this information, an investigator must understand the basics of forensic e-mail examinations.
Analyzing E-Mail Message Headers

An e-mail correspondence has two sections, the header and the body. The body of the e-mail is the message itself. If the message was used to facilitate a phishing scheme, then the body would include the link that contained the malware used for the exfiltration of the victim’s personal information. Dissecting imbedded files could also provide important electronic evidence (Schneier, 2000). While the body may reveal useful clues, the most important section of an e-mail message for tracing purposes is the header, which contains routing information to the source such as the IP address. Savvy cybercriminals can disguise their e-mail and IP addresses to prevent tracing. However, e-mail headers contain numerous sections so unless the entire header is forged, an investigator could still identify the electronic path the e-mail traveled through, including its point of origination.

The information generally found in e-mail headers is listed below. Figure 3 displays an e-mail from the author’s spam folder, which was a common solicitation for PII. The sender claimed to be from Dubai and requested bank account information in order to assist with a wire transfer for a sick relative. This is a common phishing e-mail similar to the well-known Nigerian 419 scams that are frequently found in spam folders (B. Bergiel, E. Bergiel, & Balsmeier, 2008). Each section in the diagram is labeled with the corresponding explanation listed below.
1. Return path and routing information contains the sender’s e-mail address. The address displayed here is controlled entirely by the sender and may not in any way reflect their true identity (Moore, 2011).

2. Routing information, displaying the servers in which the e-mail passed through. If several servers were involved in the transmission, then they would be displayed here in reverse order, with the last IP address being the originating one for the message (Moore, 2011).
3. DKIM identifier is the Domain Key Identified Mail signature, which is a unique digital identifier that could be used during a backwards trace through servers, particularly if the message was sent through a domain in which it did not have permission to pass in an attempt to disguise the sender (Leiba & Fenton, 2007). The DKIM could assist with locating the message when data mining a server’s administrative log. Also, DKIM may contain an embedded message from the Mail Transfer Agent (MTA), which would identify the sender’s true domain (Banday, 2011a).

4. Date and time stamp is important when tracing the IP address, particularly if a dynamic IP assignment was used by the ISP. Generally, the time zone can be determined by the number appearing next to the listed time. In the example below, the e-mail was sent on Sunday, October 27, at 9:16am in GMT 4, which is the code for Eastern Standard Time (EST) (Collins, 2006). The time zone also provides clues of the originator’s location.

5. The “from” section usually lists the actual e-mail address from the sender, although this can also be forged (Markagic, 2013). The actual e-mail address listed is mrabdul_hakim12@yahoo.co.jp, which was sent from the Japanese Yahoo e-mail service and differs from the return path. The sender used the domain Yahoo.de, which is the Duetshe version of Yahoo’s e-mail service. These are significantly different, which is likely an indication of spoofing to disguise the actual source.

6. The subject of the e-mail. If the subject in the header does not match the subject listed in the message header or includes a typo, then the header was likely forged (Banday, 2011a). In this example the subjects match.
7. Multi-Purpose Internet Mail Extensions (MIME) version that was used by the sender. In certain instances, attachments may be embedded in this and will require open source software for extraction (Banday, 2011a).

8. Message identification is a number assigned to the message and should be able to link it to its path (Banday, 2011b). The lower portion of the diagram lists the SID, or sender identification number, which also includes trace information. In this case, the SID was assigned by the AOL e-mail service to identify and authenticate the sender. ENVID or envelope identification numbers are also found in most headers (Banday, 2011a). E-mails tend to pass through servers, each of which archives a copy of it in case it fails to reach the next one before arriving in the recipient’s inbox (Moore, 2011). The servers usually add identification information, which is hidden within the identification numbers but can be retrieved with forensic software (Banday, 2011b). The Message ID, SID, and ENVID numbers are required to verify which servers the message passed through.

9. Sender policy framework (SPF) is set by the MTA and contains validation results for the domain and its servers. The validation results determine if the message met the preset policy standards of the domain owner and servers in which it passed through. In this case, the “none” indicates that AOL was unable to determine if the sender complied with the SPF, which is why it ended up in a spam folder. Most legitimate messages have permission to use the listed domain and comply with its policies. Other possibilities are “perm error,” meaning domain validation was unsuccessful or “pass,” meaning the message is in compliance with domain specifications (Banday, 2011b).
10. Finally, the body of the e-mail in text form, which would include any suspicious links or attachments that appeared in the original message. In this case, the body was redacted to save space.

Electronic messages from different e-mail services may display slightly different headers. Some e-mail services provide more header information about the message while others include less (Banday, 2011a). Regardless, the most important pieces of evidence such as the originating IP address, date and time stamp, and message identification number should appear in all e-mail headers. The sample e-mail header in Figure 3 belonged to a solicitation from a man claiming to be from Dubai who needed help transferring money. The message body requested personal information, including bank routing and account numbers, to access the recipient’s financial account. According to the header, the sender’s IP address was 50.192.164.98. A quick search in ARIN identified the IP address as originating from Miami, Florida. Interestingly, the e-mail claimed to be from a man in Dubai requesting help with a wire transfer, yet it originated in Florida.

It is possible that the registered owner of the IP address was not responsible for sending the correspondence. Knowledgeable cyber criminals are able to spoof their IP addresses or access other Wi-Fi networks without authorization to disguise their source information. In that case, an investigator should seek permission to review the administrative logs of the ISP that owns the IP address to locate any evidence of the computer that used the IP address without permission. If the header was simply forged, the IP address and corresponding ISP may not have actually been used (Markagic, 2013). Also, the message identification number and SID could assist with completing a backwards trace through the servers in which it passed as it moved from the sender closer to the recipient before landing in the inbox (Banday, 2011b). The DNS should
also be able to retrieve the original message using the identification number before the header was altered. Finally, the domain key identified mail signature could verify the originating IP address during a domain audit (Leiba & Fenton, 2007).

If the recipient fell for the phishing scam and sent their bank account information, the point of use of that PII could also assist in verifying the suspect’s location. Even if the initial activity was an electronic funds transfer, an investigator could track the funds to the point at which they were physically withdrawn or used in a debit purchase, in which case purchased merchandise would be sent to a physical address. The e-mail used for the example was an obvious phishing scam that is typically only successful 1–2% of the time (B. Bergiel, E. Bergiel, & Balsmeier, 2008). However, phishing e-mails that impersonate legitimate financial institutions, PayPal, or online retailers enjoy higher success rates (Biegelman, 2009).

**Tracing E-Mail Messages to Their Source**

Information on e-mail accounts as well as messages that were sent is archived in the servers maintained by the e-mail service, such as Google, Yahoo, and AOL. Whenever e-mail is involved in an identity theft case, investigators should serve search warrants on the designated company server to obtain any additional information on the targeted account. This investigative approach is particularly valuable during transnational or interstate investigations, where in-person follow-ups are limited. An e-mail service may also be able to provide transmission information for messages, including header information prior to alteration (Banday, 2011b).

The domain key identified mail signature (DKIM), as described in the previous example, includes a message signed by the Mail Transfer Agent (MTA), which identifies the sender’s domain. Once this information is obtained, that domain should be targeted using the message identification number to complete a successful trace. The MTA signature may not be visible in
all e-mail headers, requiring the assistance of software such as e-mail Tracker Pro, Aid4Mail forensic software, or “FINAL e-mail” (Banday, 2011b). Software programs can trace the e-mail for the investigator, simply requiring cut and pasting of the header. Deploying reliable software with a uniformed procedure can assist with maintaining the chain of custody of evidence, ensure accurate data results, and expedite the tracing process (Banday, 2011b).

While phishing e-mails often include forged headers to prevent successful tracing, suspects who simply send e-mails to confirm information for online orders or credit card applications are less likely to forge their message headers. Regardless, whenever a suspect’s e-mail account is obtained, all available information should be exhausted to assist with location identification and reveal additional schemes the individual is involved in. Another valuable piece of information that tends to be available during identity fraud schemes are mobile phone numbers, which are also subject to tracing.

**Cell Phone Forensic Techniques for Cross-Border Identity Theft Investigations**

In contemporary law enforcement investigations, cell phone data plays an increasingly significant role. Modern smartphones are equipped with Internet Wi-Fi capabilities, resembling a small computer in addition to a mobile phone. New designs also tend to include GPS functions, which provide for accurate tracing. According to data collected in 2012 by the International Telecommunications Union, 5.9 billion mobile phone subscriptions exist worldwide, indicating a high probability that law enforcement personnel will encounter such a device during an investigation. Investigators cannot overlook the potential pieces of information that could be extrapolated from mobile phone devices.
Incorporating Mobile Phone Data into Investigations

The obvious information available from either a mobile or landline phone is subscriber data. Even if a false name is provided to the carrier, how the bill is paid – through mailed paper statements or automatic draft payments from a bank account – could reveal important information to assist with identifying the subscriber. Also, when the individual began the service, they would have provided some sort of mailing address for the service provider to keep on file. Even if that address is a P.O. Box, it provides another piece of information connected to the suspect.

Some of the major challenges presented in cross-border identity theft investigations are identifying the suspect, determining their location when the point of use occurred, and assessing potential involvement in a broader criminal network. A cell phone device could assist with identifying an individual’s location at a particular day and time or unravel a complex identity fraud network. Devices could be tracked in real time and prior locations could be obtained from service providers through cell phone tower data. Tracking the device in real time could assist criminal investigators in furthering the investigation beyond a single known suspect, revealing location patterns and points of contact. The primary functions of forensic cell phone examinations during identity theft investigations are collecting and interpreting stored data, location identification, and tracking.

Data Collection and Device Tracking

Mobile phone devices can store a significant amount of information. With improved memory cards, a cell phone can store hundreds or even thousands of images, videos, documents, text messages, and lengthy call history. Cell phones equipped with Internet Wi-Fi capabilities and data plans would also contain Internet browsing history and connection sites. If data was
erased from the phone’s interface it could be recovered during a forensic analysis of the device along with information stored on the servers maintained by the cell phone provider. Obtaining server information requires a search warrant. Once the data extraction is completed, effective data mining and analysis could locate pieces of information that support an active investigation, such as e-mails sent from the phone, specific websites visited, addresses searched, or credit card information or personal profiles of victims. Identity thieves are frequently mobile, traveling to various merchants or financial institutions to avoid detection. Therefore, they are more likely to store information on portable devices such as smartphones. Some major obstacles that exist with smartphones include the security features that prevent third parties from viewing the device, since forensic software cannot override certain proprietary features on newer models (Ahmed & Dharaskar, 2008).

**Identifying the location of a device.** Cell phone tracking is a relatively new phenomenon and can be accomplished through a few methods. Most, if not all, contemporary cell phones are equipped with a Global Positioning System (GPS) capability, which refers to a constellation of 27 satellites orbiting the earth. When a device is equipped with a GPS receiver, it connects to at least three of those satellites to determine its location. This is accomplished through a mathematical concept called trilateration, which refers to determining a location based on the distance from three points (T. Wilson, 2011). For example, if a device was 90 miles from Point A, then its exact location could be anywhere within that radius, such as east or west of the point of reference. However, if it was determined that the device was 90 miles from Point A, 120 miles from Point B, and 90 miles from Point C, the additional references would narrow the location to a far more accurate position. When the points of reference are satellites, then the earth
itself can essentially serve as a fourth reference point (T. Wilson, 2011). Figure 4 provides a simplified illustration of this concept.

![Figure 4. Trilateration example. Basic illustration of trilateration using GPS from a mobile device.](image)

Cell phone developers continue to improve their devices in order to expand their market share or entice current customers to upgrade. The result has included even more accurate positioning technology that combines Wi-Fi capability with cell tower detection and GPS receivers, resulting in unusual precision. Another popular approach to locating a cell phone or verifying its previous position is through a technique known as triangulation.

**Triangulation.** The triangulation method operates similarly to GPS receivers. Mobile devices usually communicate with multiple cell towers in a local network. While the closest tower will transmit the phone call or data request, other nearby towers will pick up the presence
of the device by “pinging” it (McCullagh, 2010). By doing so, the device can move without losing reception since surrounding towers already detect its signal. Depending on the strength of the antenna, certain towers will ping devices up to 20 miles away (Parsons & Oja, 2010). Cell phone carriers record this tower information, which can be accessed by law enforcement, although such records require a judicial order or exigent circumstances. Once the cell phone provider’s records are obtained, investigators are able to analyze data regarding which towers were pinged, the direction of the antenna, and the distance from the tower (Parsons & Oja, 2010). By using multiple towers of varying strengths, an analyst triangulates the location of the device, similar to measuring the different distances from GPS satellites. If the data stretches over any period of time, changes in tower strength would indicate the direction of travel for the device. Continuing the triangulation method during the adjustments in signal strength formulates a fairly accurate location. This method is considered less accurate than GPS tracking, since static cell phone towers are less reliable than a constellation of satellites orbiting the earth (T. Wilson, 2011). Most smartphones are equipped with location software, allowing a subscriber to obtain the location of their own device; a technique often used by parents to monitor children or users to locate a lost handset device. This software could also be leveraged by law enforcement with the assistance of the provider.

**Combined tracking methods.** The most accurate method to locate a cell phone device, either during real time tracking or historical location identification, is by using a combination of the described methods. If the device is a smartphone, investigators may be able to obtain data that simultaneously locates the device based on Wi-Fi connection or data services, GPS trilateration, and tower triangulation. This concept is illustrated in Figure 5. When combined, the result is a precise location that can be used to either actively track the device or determine its
location at a specific date and time. In cross-border investigations, investigators could confirm when a phone crossed the border, whether it matches the location of an IP address during a fraudulent online transaction, or whether it was present during an in-person transaction at a store or ATM machine.

Figure 5. Cell phone pinging using multiple signal sources. Basic illustration of locating a mobile device using cell tower, GPS, and Wi-Fi signals.

Mobile Devices as a Source of Social Network Data

Mobile phones are the preferred method of telecommunication (ITU, 2012). Whether individuals are speaking during a phone call or using a Short Messaging Service (SMS) such as text messages, a record of their communication is stored. When investigators obtain cell phone records for a particular phone number, they are able to access all of the numbers that communicated with that subscriber, including SMS messages. In addition to text mining the
messages, an analyst could then use a technique known as traffic analysis. Traffic analysis is the study of communication patterns that focuses on characteristics rather than content (Schneier, 2000). Traffic analysis provides insight into social networks by understanding who communicated with whom, when, and for how long. If one member of an identity theft network is apprehended along with their mobile records, a thorough traffic analysis of call history could unravel even the most extensive networks (Westphal, 2009). Social network analysis will be explored further in the data analysis section.

**Mobile Phone Devices: Gateways to Information**

To summarize, cell phones are widely used in contemporary society and should not be ignored during investigations. The more sophisticated the device, the more information it could potentially reveal. Cell phone devices could be forensically examined for valuable information stored on them, even if the user attempted to delete it. User friendly programs exist for investigators to efficiently download data from handheld devices. XRY, for example, is a micro system software program for extracting and analyzing data from handheld devices such as mobile phones, GPS navigation units, wireless tablets, and 3G modems (Micro Systemation, 2013). When the security features of the device prevent direct data extraction, information from cell phone providers should be obtained. Mobile phones require cell towers and sometimes utilize Wi-Fi networks and GPS, which could be leveraged to identify the owner’s specific location at a particular date and time or track the device unbeknownst to the holder. Finally, social networks are generally unveiled when all of a device’s data is recovered, through phone calls, text messages, or e-mails sent from the phone.
Monitoring Wi-Fi Networks and Devices

Most citizens operate day-to-day in a highly digitized environment. Routine activities that include Internet use, cellular telephones, credit cards, and social networks provide opportunities for law enforcement to locate and track individuals (Hutton, 2007). The World Wide Web is used as a forum for transnational criminal groups to network, make contacts, recruit participants, and exchange information (Rohret & Kraft, 2011). Thus, the Internet is widely used to further cross-border identity theft schemes. Fortunately, it also presents unique surveillance opportunities to obtain information that otherwise could not be gathered strictly through physical surveillance. As law enforcement conducts successful location traces using the previously outlined techniques, the next step is to identify the specific perpetrator using the victim’s PII on the targeted network.

Internet users connect through local area networks (LANs) with either wireless or hardwire connections. The preferred method of access among consumers is wireless connectivity, in which a computer is outfitted with a wireless receiver that accesses the LAN through a wireless access point, such as a router (Anderson & Benedetti, 2009). Wireless networks by default are usually unsecured, requiring the network administrator to activate security settings, such as MAC address authentication and encryption (Whitman & Mattord 2012). Hardware and software capable of intercepting wireless transmissions are essentially the same as those required to access networks, conforming to the 802.11 standards developed by the Institute of Electrical and Electronics Engineers (IEEE) (Reyes et al., 2007). As a result, it is fairly easy to intercept Wi-Fi data. If the data is encrypted, viewing the contents could be difficult. However, decryption keys could also be obtained if the user is able to access the network itself, since it would be included in the information transmitted between authenticated
devices (Reyes et al., 2007). This section focuses on monitoring wireless networks and devices to obtain additional evidence to support an identity theft case. Utilization of these methods requires a judicial order, such as a search warrant, that documents probable cause to monitor the network or device, which otherwise would be considered an unreasonable government sponsored search in violation of the Fourth Amendment. Wi-Fi monitoring can only be carried out by Federal authorities since California wiretapping laws limit this tactic to major felonies, which does not include identity theft.

In cross-border identity theft cases, Wi-Fi monitoring will generally need to occur within the United States. Gaining lawful access to wireless networks in Mexico would require the assistance of Mexican law enforcement. However, approximately 38% of the world’s telecommunication traffic either starts or finishes in the U.S., so it is possible to intercept Internet communication that originates in Tijuana but transmits through the U.S., a justification frequently exercised by intelligence agencies (Rohret & Kraft, 2011). The most difficult step that precedes electronic monitoring is identifying the specific network or device. Law enforcement practitioners are generally prohibited from engaging in fishing expeditions where they tap into wireless networks in search of identity theft suspects without first establishing that the suspect is likely accessing the network in question. Electronic monitoring methods available for law enforcement that should be considered during identity theft investigations are packet sniffers and general Wi-Fi monitoring software, as well as keystroke loggers.

**Intercepting and Analyzing Electronic Communications**

Wi-Fi monitoring involves intercepting communications that traverse a wireless network. Wi-Fi surveillance methods include the use of packet sniffers, trap and trace, and pen registers. A packet sniffer program, or network protocol analyzer, is a tool that collects data packets
transmitted through a network and allows a third party to analyze them unbeknownst to the user (Whitman & Mattord, 2012). These programs are able to examine data from live network traffic or captured traffic and reconstruct TCP sessions (Whitman & Mattord, 2012). Packet sniffers can be customarily designed, allowing one computer to listen to multiple networks and sort the data packets accordingly (Flor & Guillory, 2011). Packet sniffers are an important component for wireless surveillance since they allow investigators to view IP headers prior to alteration. The headers and payloads recorded by the packet sniffer can then be compared to those collected during identity theft investigations to seek a match of digital fingerprints, payload attributes, or routing paths. If the packet is viewed before it reaches a proxy or anonymizer, the IP address of the intended destination should be included.

Title 18, U.S.C. § 3127 (2001) defines a pen register as, “A device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” and a trap and trace device as, “A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication.” The above federal statute also permits the use of a pen register on a web-based e-mail account to capture the IP addresses for the source and destination of the message (Buckman, 2006).

Other software programs simply record all network traffic in administrative logs. That data could be observed in progress or captured for later analysis. Monitoring live Internet traffic requires software that conforms to the 802.11 IEEE standards and is able to override security protocols that limit access. Once this is achieved, personnel can view all network transmissions
and collect evidence that demonstrates identity theft activity, such as phishing e-mails or various uses of someone else’s PII on retail and financial institution websites. Wi-Fi monitoring should include authorization to access router logs so investigators can attribute activity to specific devices through hostnames and authenticated MAC addresses using the network (Reyes et al., 2007). One major drawback with packet sniffer and general Wi-Fi monitoring programs is that encrypted data can severely inhibit payload analysis. As previously mentioned, decryption keys can be intercepted along with other traffic. If this cannot be accomplished, then other methods should be considered, such as keystroke loggers and traffic analysis.

**Keystroke logging.** One method of overcoming data packet encryption is the use of keystroke loggers in conjunction with Wi-Fi intercepts. Keystroke logger programs, also referred to as keyboard sniffers or keyloggers, record computer keystrokes for a third party to monitor specific character input (Shetty, 2010). They can be implemented as software programs or hardware devices. Once installed, these programs extract sensitive information typed into the targeted system, allowing the third party observer to decipher all Internet activity entered with the keyboard (Schneier, 2000). A keystroke logger program could record decryption keys as well as data as it is entered prior to encryption. Additionally, installing a keystroke logger program on a suspect’s computer could capture proxy web addresses, specific PII as it gets entered into fields, and communication with members of an identity theft network to expand the investigation.

The limitations associated with deploying a keystroke logging program is that an investigator would first need to identify the specific machine being used by a suspect and then figure out a method to install it without discovery. An identity theft suspect may use numerous laptop or desktop computers, resulting in missed information that could jeopardize the gathering
of pertinent evidence. Suspects could circumvent keystroke loggers by using virtual keyboards, which involve entering characters by using a mouse rather than the keyboard. Therefore, investigators using keystroke loggers should also do so in conjunction with Wi-Fi or LAN monitoring to encapsulate general network traffic.

**Traffic analysis.** When keystroke loggers are unavailable, traffic analysis should be conducted on encrypted data packets. Traffic analysis is the study of communication patterns that focuses on the characteristics of observed activity rather than content (Schneier, 2000). While traffic analysis does not cover content contained in communication, it provides the analysis of relationships by identifying with whom the targeted suspect is communicating, the length of messages, and file sizes (Schneier, 2000). Even if web activity is encrypted, the number of data packets transmitted, the size and properties of web pages, and destination of transmitted activity could provide enough information to surmise what the individual may be viewing. For example, if an intercept includes the user accessing an encrypted web page through a web proxy followed by repeated communication between two machines and then a file exchange, the user is likely engaging in an online chat with a trusted colleague. Eventually, investigators would seize any devices involved, at which point the content of transmitted information would be revealed. Recording date and time stamps is critical in order to match the traffic that was believed to be indicative of criminal activity with the contents located on the computer during a forensic analysis.

**Legal Considerations**

Wi-Fi monitoring is considered to be a form of intercepting electronic communications, or wiretapping (Moore, 2011). California wiretap laws are very strict, limiting authorization to certain felonies, among which identity theft is not included (Digital Media Law Project, 2013).
Federal statues make electronic communication intercepts more accessible with the addition of numerous qualifying offenses, including fraud and identity crimes (18 U.S.C § 2516). This framework would be most effective when utilized by an entity with Federal authority, such as the San Diego Financial Crimes Task Force. In *U.S. v. Scarfo* (2001), the FBI used a Key Logger System (KLS) to monitor a suspect’s computer. However, the FBI configured the KLS to only record keystrokes when the computer was not logged on to the Internet in order to avoid intercepting any electronic communications. Thus, the court ruled that the use of KLS to record password information was not governed under the Federal Wiretap statute. In order to obtain state approval for keystroke loggers in California, law enforcement would have to use a similar approach. In *U.S. v. Ropp* (2004), the court ruled that recording keystrokes transmitted to the computer's processing unit does not constitute an electronic communication as defined by the statute. Case law is constantly evolving as new opinions on the use of technological monitoring capabilities are formed. It is always best to consult with an Assistant U.S. Attorney or District Attorney before requesting any type of electronic surveillance activity.

**Overview of Wi-Fi Surveillance and Implementation**

Electronic monitoring of networks and associated devices can be used to gather important evidence and identify key participants in identity theft schemes. Once a device has been identified, a keystroke logger can be installed to gather passwords and encryption keys. To avoid the complications of obtaining approval for electronic monitoring, investigators should always consider simple search warrants for administrative logs from routers. If conducted immediately after a suspect has accessed the device, information close to real time would be available.

If a frequent pattern of fraudulent online transactions is established, Federal law enforcement personnel could obtain an electronic surveillance order for a Wi-Fi hotspot,
assuming the specific device can be targeted without exceeding the scope of the monitoring activity. When the suspect utilizes the hotspot, his computer’s MAC address would be recorded. Such an operation should include simultaneous physical surveillance to observe the specific time stamp of the suspect’s logon to the wireless network and visual observation of his use of the Wi-Fi. A large location would prove difficult, but a small Internet café would not. Identifying a specific local network followed by short-term monitoring, identifying the suspect’s MAC address, and then catching the suspect in possession of the computer before seizing it are generally the final steps of connecting the point of use of the PII to the perpetrator in a digitally driven identity theft investigation.

Making the Connection: Applying Data Analysis Using Link Diagrams

Data analysis is an analytical methodology that identifies meaningful patterns and behaviors within data sets (Westphal, 2009). It can be a valuable investigative tool, but is often overlooked and underutilized as a result of time constraints. However, analyzing the right data sets collected during the course of investigations could illuminate a larger picture, such as a suspect responsible for a series of identity thefts rather than the single transaction he was arrested for, or involvement in a broader identity theft network. Data analysis could also assist with identifying commonalities among various cases in the same region.

The first step in conducting data analysis is collecting and formatting the data. The best information sources at the onset of an investigation are typically the victim and whatever entities were involved, such as the online merchant that received or processed the fraudulent transaction. Merchants or financial institutions that were used by the suspect to complete the point of use stage of the identity theft may not readily release all the details, requiring a search warrant early in the investigation. Some examples of data provided by a victim include credit reports, credit
card or bank account statements, and e-mails. Merchant data includes IP addresses, phone
numbers, addresses, or e-mail addresses provided by the suspect when the fraudulent use
occurred. Once all of the information that is available at the present point is obtained, it should
be stored in a way that it can be retrieved for analysis or imported into a link diagram. If
information is provided in hard copy form, it should be scanned into a computer and then
imported into a data software program for analysis, such as Microsoft Access or Excel, Arbutus
Fraud Detection, or SAS. There are numerous other programs, and organizations should use the
one that is best tailored to their needs and familiarity. One of the most efficient methods is
creating a link analysis visual diagram using the I2 Analysts Notebook software program from
IBM.

Displaying the information using link diagrams can be extremely helpful since it provides
a visual aid for quick analysis. This technique is readily available to law enforcement in San
Diego. Law enforcement in San Diego also has access to programs that combine information
sources to query potential suspects, vehicles, addresses, stolen property, and associated
documents such as police reports. Programs such as Coplink include a function that can translate
queried results into a link diagram. Link diagrams display the results in a more meaningful way
than qualitative and quantitative data that is simply listed on a spreadsheet. Link diagrams are
also excellent visual aids for jurors to view when a complex scheme is being explained in a
courtroom. While link analysis diagrams will be demonstrated throughout this section, it should
be noted that the other software programs listed above should also be used to analyze and
manipulate data, particularly when it is first received.
Analyzing Victim Transactions for Method of Acquisition

Collecting information from victims could assist in identifying the method of acquisition by a suspect. When an identity theft scheme involves the use of a victim’s credit card, an investigator should request the last few credit card statements for the compromised account. That information should then be scanned into a computer and stored for comparison with other statements provided by victims. Different jurisdictions should always share their data to identify cross-jurisdiction schemes, which could prove especially valuable when an entire region experiences sudden spikes in credit card fraud, indicating a possible skimming device or corrupt employee scheme. An effective data analysis technique using that information would be comparing the locations of the transactions that appear on the statements to find commonalities. This can be accomplished through a software query or simply importing the data into I2 to create a diagram. Figure 6 below displays the results of one hypothetical scenario. Notice that a few locations are shared by different victims, but only one was found on all the statements, which was a gas station. Since gas stations are known to be targeted for skimming device placement, a follow up should be conducted in an attempt to see if surveillance footage still exists or if any employees may have been involved. If the commonality among the statements was a motel or restaurant, it would be an indication of a corrupt employee extracting credit card information either with a skimmer or some other artifice.
The scenarios described above could very easily be encountered in cross-border cases, as many local establishments in San Diego employ residents of Tijuana. If an individual reports being the victim of identity theft with their credit card information being used in Mexico or on both sides of the border, additional information should be gathered about their transaction habits for comparison with other cases. That information is critical when determining how to proceed after an arrest is made. An example would be an individual who is arrested after attempting to use stolen credit card information. When an identity theft investigator is notified, the credit card account is immediately connected to a skimming device scheme after the victim’s credit card statements were compared to others in the same area. While the suspect may claim this is the only identity theft he has ever attempted, the investigator already suspects otherwise. That
information would help secure a search warrant for the suspect’s residence or motel room, leading to the discovery of additional victim information and more serious charges.

**Linking IP Addresses**

Link analysis is also helpful for tracking the use of IP addresses during identity theft schemes. When an IP address is registered to an ISP in Tijuana, the privacy laws may prevent law enforcement in the U.S. from obtaining the user information behind that IP address. The solution to that challenge is a designated liaison with Mexican authorities. Assuming that is not available, it is still helpful to track which IP addresses and associated ISPs are being used in identity theft schemes. If enough incidents occur with one particular ISP, pressure from U.S. entities could disrupt their access or pressure them to provide information about those responsible for the fraudulent activity (Westphal, 2009). When the IP addresses belong to connection ports in San Diego, pattern analysis could also assist in tracking a suspect’s behavior and routines, particularly if all of the connections are made through public Wi-Fi. Some commonalities could include the same businesses such as cafés or motels being used to conduct online identity theft activities. If similar date and time stamps are discovered for the same location, then a physical or electronic surveillance operation could prove successful in identifying the suspect. Figure 7 below displays the hypothetical results of a data analysis where hundreds of cases with an identified IP address were analyzed to find which ones originated from the same address.
IP addresses that are identified as the source of phishing e-mails used to extract PII from a victim’s computer could be stored for analysis as well. That information should be shared with other agencies, particularly Federal law enforcement and task forces, to determine if it is connected to data breaches. Many phishing e-mails originate from areas far away from the victim, and thus would not fall within the scope of this regional framework. However, in some cases phishing attacks do originate in the same area as the victim and thus should be tracked. As previously mentioned, cross-border identity theft cases frequently involve electronic methods of information acquisition. If the actual links found in phishing e-mails connect to the same webhost, it could be disrupted or shut down by the U.S. or Mexican government, especially since Mexico imposes stricter Internet regulations.
Analyzing Border Crossing Information

Recall that U.S. Customs and Border Protection maintain records of individuals crossing into the United States from Mexico, and in limited cases those departing for Mexico (CBP, 2013). This information provides significant value for cross-border identity theft investigations. A suspect’s border crossing patterns could be compared to any point of use to which they are believed to be connected. The unique authority of CBP to search any individual passing through the port of entry could also be leveraged to collect valuable intelligence. Whenever a suspect in a cross-border identity theft case who resides in or frequents Tijuana is identified, an alert should be placed with CBP, instructing officers to search the individual and any electronic devices in their possession, which should include recording MAC addresses and the IP address regularly accessed. For high-value targets, an investigator may want to visit the port of entry while the individual is detained to assist with recording MAC addresses and viewing the overall findings of the search. Those results should be analyzed and compared to existing cases. If a suspect is found to be in possession of different devices each time he crosses, techniques for data storage and analysis become especially important. Figure 8 displays a sample link analysis compiling border crossing events and intelligence gathered from searches.
Analyzing Layered Schemes

Identity theft schemes are often difficult to investigate because of their complexity. Identity thieves, particularly those who operate in networks, apply a layered approach to either disguise the point of use of the compromised PII, or separate themselves from the physical location used to receive new credit cards or fraudulently purchased merchandise. Organizing information is critical to understand the roles of individuals and locations identified as the investigation progresses. Figure 9 below demonstrates layering to disguise the point of use of a victim’s PII. In this example, a gift card is purchased with a victim’s credit card information, so the suspect can use the gift card without the risk of a merchant flagging the transaction.
Identity theft perpetrators who place online orders using a victim’s credit card or receive a new credit card under the victim’s name need a mailing address. These are frequently P.O. Boxes, unoccupied homes, or residences of people who agreed to receive the items on the suspect’s behalf. Frequently, those who claim the items are not the person who placed the order. This method provides a layer of protection, should law enforcement become aware and detain whoever is seen retrieving the items (Collins, 2006). Thus, while investigators need to identify that individual, they may not wish to arrest them, but rather continue the surveillance until they are led to the primary suspect. That process could become complicated, particularly if the initial person visits several individuals. Figure 10 below provides a hypothetical diagram created from surveillance notes after an investigator enters information about the people and places observed during an operation. The result is a quick reference for other personnel who may be assisting with the investigation to track the information gathered.
The above diagram could easily be expanded as additional attributes are identified. This diagram would serve as a visual aid as investigators evaluate all of the evidence gathered to determine if all relevant parties participating in the scheme have been identified.

**Using Social Network Analysis to Unravel Identity Theft Networks**

Criminal networks that facilitate large-scale identity theft schemes tend to span local jurisdictions or even various countries around the globe (Coggeshall, 2012). Some of these networks operate with centralized control, while others are loosely connected and exist mainly to share victim information, law enforcement tactics, and techniques to further schemes (Amerding, 2012). Disrupting networks could significantly improve clearance rates, attributing dozens of cases to one core group of individuals. At the onset of an investigation, the primary sources of information are the victim and entities involved in the point of use of the PII. However, as the investigation progresses and an individual is identified or apprehended, that suspect becomes the most valuable source of information. Therefore, law enforcement should maximize the value of
each arrest by determining whether the defendant was a single actor or connected to a more
organized network of identity thieves, and if so, what their role was within that network. This
process usually begins with a forensic analysis of the subject’s cell phone and computer,
determining who was communicated with and how often. Once all of the available data is
collected, an effective technique known as social network analysis (SNA) can be instituted.

**Social network analysis with call records.** Social network analysis is an analytical
approach that examines and maps social relations to identify criminal networks (Johnson,
Reitzel, Norwood, McCoy, Cummings, & Tate, 2013). Continuing with the link analysis model,
data such as lengthy call logs could be imported into the I2 software program to display the
amount of traffic occurring between the suspect’s cell phone and those found on his call list. This
data should be collected from the service provider to capture data deleted from the phone. Recall
that traffic analysis examines the characteristics of calls rather than the content. By simply
identifying phone numbers that a defendant regularly communicates with, investigators could
ascertain additional targets to expand their investigation. Once those individuals are identified,
even if only by first name or moniker and phone number, additional research in law enforcement
databases could reveal their entire identity, particularly if any of their attributes have been
connected to previous investigations. Figure 11 is a sample display that could be assembled
using data from a contact list on a cell phone. The thicker lines indicate a higher volume of calls
exchanged.
Cross-referencing suspects with call and text records. Figure 12 illustrates basic traffic analysis for phone numbers and text messages. Once again, the links are weighted to display the higher frequencies of contact. An actual link diagram containing real information should substitute the icons for any available photographs of the people they represent along with other attributes such as name, nickname, phone number, address, and birthdate. The icons in figure 12 that are flagged are the subjects of other identity theft investigations. Normally, contacts associated with any other open case should be indicated in the diagram. For example, a suspect of a vehicle burglary who regularly contacts the suspect may be providing personal information taken from those thefts.
Based on the display in figure 12, an investigator could quickly observe important characteristics, such as the fact that contact 1 is not only the subject of another investigation, but the suspect communicates with him mostly through text messages. Contact 9, who is also involved in another investigation, has a thicker link on the mobile phone portion but is non-existent among the text message data, indicating that the suspect communicates with this person solely through phone calls. In addition to phone numbers, communication between computers is also important to analyze. File sharing is common within identity theft networks, as suspects distribute or trade profiles containing victim information. This type of information more directly indicates involvement in identity theft activity. As a result, it can be more difficult to obtain such identifiers, as most communications are encrypted and pass through anonymizers. However, the
information found on the subject’s computer should be compared with information used by other suspects, since any matches could indicate a connection.

**Centrality and hierarchies.** Social Network Analysis seeks to classify the roles and importance of people or places in a network, identifying key actors in complex groups to determine centrality and information flow (Schwartz & Rousell, 2009). SNA can assist with measuring the depth of a network and relative connectedness of participants, as well as identifying cliques or subgroups (Westphal, 2009). Ascertaining the path of information flow is especially important. For example, if information regularly originates from various sources only to condense as it funnels through a few individuals to reach one person, then that is indicative of a hierarchy structure, which is displayed in figure 13 below. Notice that the flow of information becomes more organized with the higher levels. This concept is known as centrality, which exposes a high degree of centralized control (Westphal, 2009).

![Figure 13. Sample hierarchy. This figure illustrates a network with a high degree of centrality.](image)
Investigators tend to find members of the lower levels first, as those situated higher are more protected. Analyzing the communication among the lower-level participants in this model may appear confusing and difficult to attribute to an organized network, demonstrating the utility of visual aids. Discovering the true hierarchy structure is the first step to identifying the leadership, who would then be targeted to disrupt and dismantle the network altogether.

**Closeness and betweenness.** Figure 13 shows a basic hierarchy that, once displayed in a link diagram, clearly illustrates the individuals with centralized control. Figure 14 below, however, displays more complex patterns of communication. Assume this diagram was created after importing an excel file containing cell phone data among suspects into the I2 Analyst’s Notebook software.

![Complex identity theft network](image)

*Figure 14. Complex identity theft network. This link diagram illustrates data of contacts among members of a criminal network, where the hierarchy is less clear.*

The individuals are clearly connected, but who ultimately controls the flow of information? To obtain the answer, an investigator should calculate betweenness and closeness. Betweenness
reveals the subjects in the network with the most links, identifying those who tie together the largest number of routes (Westphal, 2009). Closeness calculations yield the people in the network that are most interrelated and potentially possess the highest degree of control within the network (Schwartz & Rousell, 2009). The I2 Analyst’s Notebook software instantly calculates those concepts for the user. Table 1 displays the top 5 subjects from the results of those calculations.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Betweenness</th>
<th>Closeness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person 16</td>
<td>25%</td>
<td>79%</td>
</tr>
<tr>
<td>Person 12</td>
<td>61</td>
<td>90</td>
</tr>
<tr>
<td>Person 7</td>
<td>100</td>
<td>95</td>
</tr>
<tr>
<td>Person 2</td>
<td>8</td>
<td>65</td>
</tr>
<tr>
<td>Person 1</td>
<td>84</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 1. Results of betweenness and closeness calculations for top 5 subjects, displayed by percentage.

The betweenness score indicates the percentage of people in which that subject has contact with; the closeness score relates to the percentage of relationships the subject has with the other network participants (Westphal, 2009). According to the results displayed in Table 1, Person 7 is likely the centralized source of information within the network, having contact with 100% of the participants, followed by person 12. An investigator in this scenario should conduct traffic analysis among those five individuals, focusing on the frequency of contact between Person 7 and Person 12. Figure 15 displays the results within the link diagram, providing a quick reference for the investigators tasked with investigating this network and the complex schemes they may be involved in.
Interestingly, the results from Table 1 show that Person 2 does not have a high degree of betweenness in comparison to the other four listed. While Figure 15 displays regular contact between Person 2 and three out of the other four subjects, he may only possess limited information regarding the remaining participants in the network.

Closeness and betweenness are important concepts when conducting SNA since they identify the most probable central figures in networks that are otherwise not centrally organized. Apprehending those individuals could result in disrupting the entire network and identifying most if not all of the remaining participants. Finally, proving an organized effort by demonstrating the patterns of behavior and communication could result in more serious charges for participants such as conspiracy and racketeering (Collins, 2006).
The Importance of Data Analysis

Suspects involved in cross-border identity thefts frequently involve friends or family members on both sides of the border, so social network analysis is an important technique that should be considered with anyone that appears to operate with even a hint of sophistication. Which members communicate directly and how information flows are basic concepts that can provide significant insight into how a group operates. Verifying interpretations and theories that result from SNA should always be attempted by analyzing conversion scripts such as text messages, e-mails, or wiretap recordings, or reviewing interview notes of suspects (Campana & Varese, 2012).

Monitoring and disrupting identity theft networks yield the greatest benefit for investigations; however, networks are frequently well organized, deploy layers to protect their hierarchy, and are familiar with police tactics. Therefore, it is difficult to assemble an operation that will dismantle the entire network from onset. Rather, investigators should seek to maximize the value of each arrest by assessing whether an individual appears to be part of a network, and if so, gather that individual’s contacts from their electronic devices. Then, they can conduct intensive but efficient research on those contacts to identify others involved followed by evaluating other cases and persons targeted for investigation to determine if they somehow relate to the individual in custody. Identity theft cases, particularly networks, can be tedious and time consuming. Effective data analysis techniques can reduce time and improve efficiency, yielding valuable results that will further an investigation.

Data analysis techniques assist with tracking the progress of identity theft investigations and sorting through layers in complex schemes. Identity thefts may support other crimes, or be the chosen method that a career criminal uses to earn their living or support a drug habit.
Regardless, effective data analysis will help to maximize the value of each arrest and connect individuals to as many cases as possible resulting in improved clearance rates and identification of additional suspects. The intelligence available through data analysis is often overlooked by investigators inundated with cases; however, it is invaluable and should be included in every investigator’s toolkit.

**General Recommendations**

**Addressing Cross-Border Identity Theft with a Holistic Approach**

Effective strategies that prevent and deter identity thefts tend to include a holistic approach, enlisting cooperation between private and public sector entities. This investigative framework requires a similar level of inclusiveness. The previously discussed cyber investigative methods, particularly data packet tracing, have proven to be an effective procedure for tracing the source of network activity when properly executed. Applying such a cutting-edge technique to identity thefts can be equally successful. However, actual implementation could prove to be difficult. Online merchants and financial institutions need to be aware of this goal and configure their networks to extract and store data packet headers. While many large companies already have this capability as part of their cyber security protocol, some may not be prepared for such a request by law enforcement personnel. Therefore, communication between investigators and IT personnel is important. Members of a company’s IT staff should be prepared to provide the necessary information upon request. Furthermore, they should assist investigators with the tracing process, ensuring all available information is leveraged. This inclusive strategy would ensure proper implementation of data packet tracing.

Another important step is requiring more information for authentication. Entities engaging in e-commerce should require valid phone number and e-mail address along with the
shipping address. An electronic address from an anonymous e-mail service should automatically result in a rejected order. This would increase the likelihood of a traceable e-mail address or phone number being provided. The President’s Identity Theft Task Force should also communicate the importance of assisting law enforcement with executing data packet tracing and requiring authentication for online merchants. The U.S. government could especially compel federally regulated banks to comply. This holistic approach would significantly increase the likelihood of successful IP tracing and location verification tactics, enhancing law enforcement’s ability to investigate cross-border identity thefts that are electronic in nature.

**Partnering With Mexico**

Any strategy that addresses cross-border crime with Mexico requires close partnerships. Most law enforcement agencies that operate within the border region with Tijuana maintain communication with their Mexican counterparts, usually through a liaison. Currently, most partnerships are centered on drug trafficking, money laundering, human smuggling, kidnapping, and arms trafficking. In order to extend the reach of U.S. law enforcement to identity theft suspects in Mexico, law enforcement south of the border must be available and willing to assist. By doing so, the techniques outlined in this paper will be far more effective. U.S. investigators working closely with Mexican officials could trace IP addresses, track deliveries from online orders, and conduct surveillance in Tijuana. They would also have access to ISP records and IP address locations.

The review of the literature mentioned a bilateral agreement between the U.S. Government and Profeco, Mexico’s consumer protection agency, to address cross-border fraud. This should be taken a step further to create a Mutual Legal Assistance Treaty (MLAT) specifically for identity theft and cross-border fraud cases. The MLAT should include
agreements to assist in information gathering and intelligence collection as well as extradition of identity theft suspects who reside in Tijuana or seek refuge there. Currently, Mexico participates in MLATs with numerous countries, including the U.S., to assist with money laundering and drug trafficking investigations (Financial Action Task Force, 2008). While this proposal is of a much smaller scale, it should be fully supported by Mexico’s centralized and local governments. Major U.S. banks and corporations have extended services into Mexico, so a legal agreement that lifts restrictions on cross-border identity theft investigations is long overdue to protect consumers, employees, and company assets. It would also outline specific protocols and training for U.S. personnel operating in Mexico as advisors to their counterparts.

**Practical Application: Hypothetical Scenarios**

The following scenarios are based on cross-border identity theft cases that occurred in San Diego. Actual names of persons, entities, locations, and dates were redacted for privacy purposes. While the modus operandi is based on fact, the solutions are fictitious and should not be accepted as the actual result. Rather, these scenarios are intended to demonstrate the use of the recommended methodologies outlined in this project. Each scenario begins with a brief description of the scheme followed by a realistic solution.

**Scenario 1: “Two free nights at a motel… with a gift card?”**

**The scheme.** A suspect in obtains a victim’s credit card information using a phishing e-mail sent from an IP address in Tijuana. The discovery occurs when the victim, who resides in San Diego, notices that a $500 prepaid Visa gift card was charged to their credit card in Tijuana, Mexico. Investigators contact Visa, who informs them that the gift card was then used to purchase five more gift cards of $100 each, with the activation fees being paid with cash. Any subsequent point of sale transactions with those gift cards will directly relate to the initial
identity theft. However, merchants processing those sales, whether online or in-person, are unlikely to flag the transactions.

**Possible solution.** In order to obtain gift card transactions, investigators serve a search warrant on the issuing bank that includes monitoring instructions. For the purpose of this scenario, assume the card issuer is simply Visa rather than a bank. Visa places a fraud alert on those cards, requesting notification of their fraud unit whenever they are used since it is unclear whether the subsequent gift cards were distributed to different people or held by the initial suspect. Complying with the court order, the Visa fraud unit contacts the assigned law enforcement investigators when one of the prepaid cards is used to purchase two nights in a motel in San Ysidro. A telephonic search warrant for the room is obtained. During the search, officers and investigators locate a laptop, mobile phone, and a dozen gift cards, including the ones connected with the scheme. The individual staying in the motel room is arrested. He claims he bought the cards for $50 each in Tijuana from a man whom he only knows as “George.”

A forensic examination of his laptop uncovers the victim’s credit card information used to purchase the initial $500 gift card. His mobile phone is also examined and text messages requesting prepaid gift cards are discovered with negotiated prices. Those numbers are collected and the cell phone account holders become targets of additional follow-ups. All of the e-mail accounts the man utilized are identified and search warrants are served on the client servers. The results yield hundreds of phishing e-mails sent to various victims. As a result, the man is connected to dozens of additional identity thefts and appropriate charges are added, preventing his immediate release from jail. The man states he sent all of the phishing e-mails from Tijuana in order to prevent U.S. law enforcement from tracking him. He adds that he liquidated most of the gift cards that he bought with victim’s credit card information by selling them at discounted
prices on both sides of the border to implement additional layers from the initial fraudulent transactions; when buyers were not readily available he spent the prepaid cards himself. Figure 16 illustrates a link diagram that would assist with summarizing and tracking this investigation as it expands to additional suspects.

Figure 16. Scenario 1 link diagram. Tracking and summarizing the scheme as the investigation expands.

Scenario 2: “Give him credit”

The scheme. Local law enforcement in San Diego receives a report from another agency in Northern California. The report states that a small business owner was contacted by a large software company inquiring about his recent order on his credit account. The man was stunned since he never opened such an account. The company informed the man that about $10,000 worth of hardware and software were ordered, with a shipping address in San Ysidro, the border neighborhood in San Diego. The man immediately obtained his credit reports and noticed the suspicious credit account in addition to new credit cards; all of which were opened with his and his wife’s PII, listing the same shipping address. When he contacted the credit card issuer, he
found that over $700 in cash advances were completed in Tijuana. The man reported the crimes to his local police department, who then forwarded the report to their counterparts in San Diego. Criminal Investigators in San Diego discover the address used for each account was a P.O. Box located near the San Ysidro Port of Entry, which is commonly utilized by Tijuana residents who take advantage of the more secure postal service in the United States. The name registered with the box is falsified along with the associated physical address in Tijuana. The IP address captured by the online retailer is provided, which traces to an ISP in Zona Norte, a section of Tijuana just south of the San Ysidro Port of Entry.

Possible solution. Applying the framework from this project, the first step would be to extract all available information from the points of use of the victim’s PII, which can be broken into three parts:

1. The online order
2. The credit applications
3. The credit card transactions

The same cell phone number and e-mail address were used when the credit accounts were opened, only to eventually be canceled, ruling out the possibility of active device tracking. However, historic cell tower information would demonstrate the suspect’s movement before cancelling the phone service. The IP address captured for each credit card application matched the one used earlier in Tijuana. Search warrants are served on the cell phone carrier, e-mail service, and credit card issuer for all available account information. The cell phone was used several times to call a landline subscriber in San Ysidro, which indicates a family member or friend. Historic cell tower information places the mobile device at that location shortly after a call was made. The credit card issuer reports an additional online order that was placed but
not completed since it was flagged. That merchant is immediately contacted by investigators and connects them to the IT department. The captured IP address differs from the one used to complete the credit applications. The data packet associated with the activity on the merchant’s network is retrieved and the IP header links to a router in San Ysidro, which matches the landline that the suspect called with his cell phone. Investigators question the resident, who believes the suspect is a family member who resides in Tijuana. The resident consents to a search of their router log, which identifies the suspect’s MAC address, based on date and time stamps from the online order.

Investigators place an alert on the suspect’s vehicle at the San Ysidro Port of Entry. When he reenters the U.S., CBP officers detain him and search his computer and mobile devices. The man is in possession of numerous phones, one of which he maintains permanently while the others he lists for online orders only to discard shortly thereafter. Investigators are notified and seize the computer for forensic examination. A brief field search of the laptop recovers cookie files, which are placed on a hard drive by web pages for faster connection when the user revisits the page (Beal, 2008). Those files match the most recent identity theft transaction, as well as hidden files containing PII profiles and credit card information. The subject is arrested. A forensic examination of his primary cell phone uncovers a web of contacts, some of which have extensive criminal history of drug use and identity theft charges, indicating a possible cross-border network. The man stated he uses a P.O. Box in San Ysidro, but frequently pays someone else to retrieve his packages, layering himself from the physical location.
Scenario 3: “Malicious funds transfer”

The scheme. Police are called to a business in San Diego to complete a theft report. One of the employees explains that $300,000 was transferred from their business account to a personal bank account held by, “Tommy Rodriguez,” which they believe to be an alias. Embezzlement is ruled out, as only a handful of employees have access to the company’s financials. The company retains a computer forensic expert who discovers malware on the server and believes it was used to extract account information, including passwords. E-mail logs are reviewed and a phishing message is discovered that included a link containing the malware file. This case serves as an example where a business was the victim of identity theft as a suspect was able to misrepresent himself as an employee to the company’s bank, completing an electronic funds transfer.

Possible solution. Identity theft investigators conduct forensic examinations of the e-mail and associated data packets that traveled through the company’s server, which trace to an IP address in Tijuana. They then consult bank personnel, who provide the IP address from which the account itself was accessed along with associated date and time stamps. That IP address traced to a Wi-Fi hotspot, a Starbucks café located in the border region of San Diego. Additionally, a few thousand dollars were withdrawn shortly thereafter from a nearby ATM machine using a debit card from the suspect’s account. A few hours later, another ATM withdrawal occurs at a gentlemen’s club in Tijuana. The destination account belonged to a subsidiary bank of a U.S.-based institution. As with the actual case, the bank freezes most of the funds before they were moved again. Surveillance footage from the ATM in San Diego captures an image of the suspect. U.S. officials contact their liaison in Tijuana to investigate the registered
owner of the IP address through the associated ISP, only to discover that local wireless network was used by an unknown third party.

A search warrant is served on the bank to obtain the signature card that was created when the account was opened, revealing a fake Baja California identification card and stolen passport number. Bank personnel agree to create a ruse with criminal investigators and Tijuana officials, inactivating the man’s debit card and instructing him to visit a branch for a new one, which the man refuses to do. Investigators also obtain a warrant to place a pen register on the man’s e-mail service, to record his IP address whenever he logs in to his account. The investigators are notified when his e-mail is accessed from an IP address at the same Wi-Fi hotspot in San Diego. While in possession of the earlier photograph, a surveillance operation is quickly deployed. When a man matching the description in the photograph leaves the location, he is detained and his laptop is searched. Files are located connecting him to the electronic funds transfers, along with several additional bank accounts. He is also in possession of falsified identification cards and passports. A more in-depth forensic analysis of the man’s laptop reveals the malware file along with additional e-mails that were sent to other companies. Investigators contacted those companies, a few of which were also victimized, strengthening their case.

**Potential Framework for Success**

The above scenarios began based on actual cases but were not actually solved since the above techniques were not utilized. While it is unlikely the scenarios would play out in that exact manner described, they are intended to demonstrate how this framework could potentially be applied in combination with current investigative techniques. More advanced methodologies would logically improve the probability of identifying suspects in cross-border identity theft.
schemes, particularly as law enforcement faces unconventional tactics deployed by criminals to avoid detection.

**Conclusion**

This project explored the challenges of cross-border identity theft investigations, focusing on the San Diego–Tijuana region. General data about identity theft and cross-border fraud trends suggests that these crimes are digital in nature, taking advantage of the anonymity provided by the Internet. Advances in e-commerce technology were accompanied by sophisticated fraud schemes as opportunistic criminals sought new methods of obtaining illicit funds. The new phenomenon of cyber-based criminal activity exposed an unprepared law enforcement community, particularly traditional entities unaccustomed to digital forensic methodologies. This limited the response to identity theft investigations while increasing the success rate of identity theft schemes. Without capable and willing investigators pursuing identity theft suspects, that negative trend will only continue.

As a result of the digital nature of cross-border identity thefts, the research for this project focused on cyber investigative methods. The most significant challenge is tracing the online activity to a location in order to identify a suspect. Thus, significant attention was paid to tracing IP addresses, data packets, e-mail messages, and mobile phone numbers. These techniques, with the exception of the latter, are not widely exercised within the local law enforcement community. Another effective tactic is Wi-Fi surveillance through trap and trace devices and pen registers. In order for these to be deployed in the San Diego–Tijuana region, they would have to be initiated under the Federal wiretap law as California limits wiretapping to significant felonies. Finally, data analysis using link diagrams are an effective method to track investigations and locate investigative leads within large data sets.
When combined with the proper personnel training and user-friendly software, the aforementioned techniques create a comprehensive framework that not only guides law enforcement through what were once considered unsolvable crimes, but holds the potential to connect the point of use of a victim’s PII to a perpetrator with each case. While certain cases may remain unsolvable, many will lead to a more favorable conclusion, improving law enforcement’s ability to respond to reports of cross-border identity thefts. Challenges will certainly arise as the techniques are implemented. However, by combining local and Federal resources, facilitating partnerships with banks and private sector retailers, and ensuring a cooperative approach with Mexican authorities, law enforcement in the San Diego–Tijuana region will attack the identity theft epidemic in ways never experienced before, setting an example for the entire country.
References


United States v. Scarfo. 180 F.Supp.2d 572 (District Court, N.J. 2001)


