

I. Problem Statement

Overview

Compared to previous generations, the Post-Industrial, Information Age of the 21st Century Western Civilization has made life, work and recreation more enjoyable, much easier and has considerably advanced the affluence of most people's lives in modern society. The materialism of the 21st century combined with the financial by-products of increased affluence among the masses allows individuals or entire families to go to work, attend college for several years, travel local or worldwide for business or leisure and stay at five-star hotels, eat three-plus meals a day and enjoy recreational activities only dreamed about by past generations – all without any money. Every transaction can literally be put on their “tab”, either charged to a credit card or debited automatically from a bank account. For the few people who lack a credit or debit card, or whose cards are maxed out, instant credit – pre-approved and mailed right to their door – fills the gap.

When it comes to enjoying the good life, it takes sophisticated technology to make it happen. In past generations, the necessary technology was unavailable or at least out of the reach of the common person. But in contemporary America you can buy an enormous amount of technology at your local shopping mall. Because of this, a lot of devices are commonly available that could collect, contain and alter electronic information. For example, consider a Microsoft® Xbox® or other gaming system. For as little as \$30, one can modify it to use Linux®. At this point it could become a fully functioning file server, e-mail server, and/or peer-to-peer server and subsequently it could be utilized to store any type of material, whether legal or illicit.¹ In addition, memory cards the size of a postage stamp can hold up to three times the information stored on a CD-ROM. The chip may be so small that it can be hidden on the corner of a desk and easily be out of sight under a knickknack, or even mistaken for one.²

The American economy generates an enormous amount of data. Most users of that information are from honest businesses getting and giving legitimate information.³ However, the same advancements in technology that allow people in modern society to enjoy “the finer things in life” have also made life easier and more profitable for criminals, especially those so-called *White Collar Criminals*. Gone are the days when someone walks into a bank and says “Hello, I’m Clyde Barrow and I’m here to rob you. Now give me all of your money” and then they keep robbing banks until the F.B.I. comes out and shoots them. Now-a-days the tools of the trade for serious criminals are a computer, mailbox and sometimes an ink pen. In fact, if a contemporary crook is armed with the right information, no “tool” is required. In contemporary Western Civilization, information – and knowledge – truly is power. And, in a drastic change from past generations, instead of robbing a bank between 9 & 5, contemporary crooks often hit it in

¹ Information Hide and Seek. Tech Beat. Summer 2005.

² A Small Matter of Size. Tech beat. Spring 2005.

³ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. P 9.

the middle of the night while it's closed. The modern crook can literally steal millions of dollars without speaking to anyone at a financial institution or even entering onto the property.

Not only are corporations and lending institutions prime targets for contemporary crooks. Savvy criminals have identified another target which - although having less total wealth than a mega-corporation – almost always proves to be an easier target: **the private citizen.**

The 1990's spawned a new variety of crooks called *identity thieves*. Identity thieves comprise a major subset of white collar crooks and they perpetrate a tremendous amount of fraud against major corporations and private citizens. Their stock in trade is the everyday business transaction. Each transaction requires one to share personal information: bank and credit card account numbers; income status amounts; Social Security numbers (SSN); or name, address and phone numbers. An identity thief co-opts some piece of this personal information and appropriates it without one's knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses someone's personal information to open a credit card account in their name.⁴

Oftentimes, individual proprietary information necessary for a legitimate transaction to occur is contained several times over in the small electronic documents carried in purses and wallets. The same (and additional) information is also stored in many different databases in the United States and worldwide. The information required to execute a legit transaction is the same information this is used by white-collar criminals to "clean out" an unsuspecting victim. Credit and debit cards provide a wealth of information about private individuals. Many other forms of financial exchanges, including pre-approved loans hold that same information. The data encoded in these documents can be decoded by sophisticated criminals. The documents themselves can be altered by a crook with average intelligence or used in their original form by a typical less-sophisticated crook.

In corporate America the terms "White Collar Crime" and "Financial Crimes" have become synonymous. How should white-collar crime be defined and why do we make a distinction between embezzlement by a corporate executive and "street crimes" such as theft, drugs, and prostitution? There are no easy answers to these questions. Although white-collar crime has a long history, it has received little attention because violations, violators, and victims are often unclear. One thing that is clear is that the incidence of white-collar criminal activity is on the rise in the United States and it threatens the economic health and stability of the nation. In addition, white-collar crime has been correlated with other types of crimes that are acutely detrimental and chronically devastating to society. Some of the *blue collar* criminal activity that has been correlated with white collar crime is drug trafficking, human trafficking, (modern-day slavery), weapons trafficking, car theft rings and terrorism. All of these crimes have been further correlated with additional acts of violence perpetuated against the victims and society as

⁴ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. P 1.

a whole. Moreover, all of these crimes require the perpetrator to travel and make financial transactions with someone else's (or a fictitious) identity.

The idea of white-collar crime was first introduced by Edwin H. Sutherland during his presidential address at the American Sociological Society Meeting in 1939. He raised concern over the criminological community's preoccupation with the low status offender and "street crimes" and the relative inattention given to the offenses perpetrated by people in higher status occupations. In his book, *White Collar Crime*, Sutherland explained further that white-collar crime "may be defined approximately as a crime committed by a person of respectability and high social status in the course of his occupation" (p. 9). Unfortunately, this definition seemed to spark more debate rather than further delineate the range of criminal behaviors that constitute white-collar crime. People continue to focus on the word "approximately" and use that as a basis to stretch or shrink the scope of white-collar crime to serve their purposes.⁵

Currently, the definition of white-collar crime is still hotly contested within the community of experts. Although there is a multitude of variations, there appears to be three major orientations: those that define white-collar crime by the type of offender (e.g., high socioeconomic status and/or occupation of trust); those that define it in terms of the type of offense (e.g., economic crime); and those that study it in terms of the organizational culture rather than the offender or offense. Additionally, there are also those that confine the definition mainly to economic crime, as well as others that include other corporate crimes like environmental law violations and health and safety law violations.⁶

The Federal Bureau of Investigation has opted to approach white-collar crime in terms of the offense. The Bureau has defined white-collar crime as

“. . . those illegal acts which are characterized by deceit, concealment, or violation of trust and which are not dependent upon the application or threat of physical force or violence. Individuals and organizations commit these acts to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure personal or business advantage.”

Some experts have criticized defining white-collar crime in terms of type of offense because this definition emphasizes the nature of the acts rather than the background of the offender. Within the FBI definition, there is no mention of the type of occupation or the socioeconomic position of the "white-collar" offender.⁷

⁵ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

⁶ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

⁷ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

Although it is acceptable to use socioeconomic characteristics of the offender to define white-collar crime, it is impossible to measure white-collar crime with UCR data if the working definition revolves around the type of offender. There are no socioeconomic or occupational indicators of the offender in the data. Additionally, there are no measures of corporate structure in UCR data elements. Given that, research using UCR data must approach white-collar crime in terms of type of offense.⁸

In victimology, blue-collar crime affects more obvious victims who report the crime, whereas in the corporate world, the identification of a victim is less obvious and the issue of reporting is complicated by a culture of commercial confidentiality to protect shareholder value. It is estimated that a great deal of white collar crime is undetected or, if detected, it is not reported.

The types of crime committed by criminals are a function of the opportunities available to the potential offender. Thus, those at the lower levels of society and living in inner-city areas as well as those employed in relatively unskilled environments have fewer "situations" or opportunities to exploit than those who work in "situations" where large financial transactions occur and live in areas where there is relative prosperity. "Blue-collar crime" tends to be more obvious and attract more active police attention (e.g. for crimes such as vandalism or shoplifting which protect property interests), whereas white-collar employees can intermingle legitimate and criminal behavior and be less obvious when committing the crime. Thus, blue-collar crime will more often use physical force whereas white-collar crime will tend to be more technical in nature, e.g. in the manipulation of accountancy or inventory records.

The common thread in white-collar crimes is the assumption of proprietary information to commit or facilitate the crime, i.e., almost always, identity theft. For instance, in order to defraud a bank one must pose as somebody else in order to misappropriate the other person's proprietary accounts. For that reason this paper will focus on identity theft and fraud as the nexus between most white collar criminal activities.

According to the United States Secret Service, White Collar Crime consists mainly of Identity Theft, Check Fraud, False Identification, Bank Fraud, Access to Vice, Passport/Visa Fraud, and Credit Card Fraud. Other research indicates that some additional related crimes are Forgery, Credit Card Theft, Financial Identity Theft, Breach of Trust (employee / employer relationship), Internet Fraud, Internet Gambling, Insurance Fraud and Computer Crimes (a.k.a. *cyber crime*⁹). For simplicity, in this document, some of the crimes may be pooled together. For instance, Financial Identity Theft & I.D. theft will be considered as one crime and Bank Fraud, while in many instances not specifically referenced or covered in detail, will be assumed to be included in a group with several other types of crimes.

⁸ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

⁹ For the purposes of this document, Computer Crime and Cyber Crime may be used interchangeably.

The United States Secret Service has identified Identity Crime as *A theft or misuse of personal or financial identifiers in order to gain something of value and/or to facilitate other criminal activity*. Identity Crime is not simply taking over or using someone else's identity. It is the actual use of the identity for *criminal purposes*.¹⁰

Identity theft occurs when a person uses someone else's name or personal information, such as one's social security number, driver's license number, credit card number, telephone number or other account numbers, without one's permission. Identity thieves use the personal information to open credit, bank and telephone service accounts, and to make major purchases – all in the victim's name. Information can be used to take over the victim's existing accounts and/or to open new accounts. Identity theft can result in damage to the victim's credit rating and denials of credit and job offers.¹¹

Computer usage in white collar criminal activity

There appears to be strong nexus between financial crimes and cyber crime, in fact they overlap significantly. It's called electronic crime, or e-crime. The weapon is a computer, the scene of the crime can be a hard drive, and the perpetrators and victims can be thousands of miles apart. It can involve identity theft, financial misappropriation, privacy invasion, child pornography, or intellectual property theft. Because of jurisdictional constraints it often renders law enforcement agencies helpless.¹²

Since the information technology revolution began, law enforcement has faced the growing problem of cyber-crime. But a lack of resources and trained personnel has put many agencies behind the curve. Along with trained personnel to investigate such traditional crimes as murder, arson, theft, and assault, law enforcement needs specialized cops trained to fight financial crimes committed electronically.¹³

In the cyberworld of home or office computers, a concept known as “metadata” comes into play. Metadata is information stored below the surface of documents, spreadsheets, and presentations created online through commonly used office productivity suites. Because this hidden data resides out of the visible interface, few users are aware that it is there. Metadata can contain personal information about the author of a file and the computer or network from which it was stored, saved, or printed. It can catalog e-mail addresses, the last 10 people who viewed the file, and/or *past versions of the document*. According to a researcher from the National Institute of Justice's CyberScience Laboratory in Rome, New York, the release of such metadata can be a starting point for hackers or divulge sensitive information to those who should not have it. The improper release of metadata has caused embarrassment, resulted in the loss of intellectual property, influenced the outcome of legal proceedings, and even endangered lives.¹⁴

¹⁰ Secret Service Digital Lecture included on RULETC CD. Gatlinburg Law Enforcement Conference. May 2006.

¹¹ IDENTITY THEFT: Reduce Your Risk. American Express. (Pamphlet)

¹² Cyber Cops in Training. Tech beat. Winter 2004.

¹³ Cyber Cops in Training. Tech beat. Winter 2004.

¹⁴ Technology Primer: Data...About Your Data. Tech Beat. Season 2005.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years - and thousands of dollars - cleaning up the mess that thieves have made of their good name and credit record. In the meantime, victims may lose job opportunities, be refused loans for education, housing, cars, or even be arrested for crimes they didn't commit. Humiliation, anger and frustration are common feelings victims experience as they navigate the arduous process of reclaiming their identity.¹⁵

Unlike victims of other crimes, who generally are treated with respect and sympathy, identity theft victims often find themselves having to prove that they're actually victims and not deadbeats trying to get out of paying bad debts.¹⁶ A consumer complaint filed with the Federal Trade Commission on January 2, 2001, indicated that a lady's purse was stolen in December 1990. Subsequently, in February 1991, she started getting notices of bounced checks. About a year later, she received information that someone using her identity had defaulted on a number of lease agreements and bought a car. In 1997, she learned that someone had been working under her Social Security number for a number of years. A man had been arrested and used her SSN on his arrest sheet. There's a hit in the FBI computers for her SSN with a different name and gender. She can't get credit because of this situation. The victim has been denied a mortgage loan, employment, credit cards, and medical care for her children. She has even had auto insurance, medical insurance and tuition assistance denied.¹⁷

Definitions¹⁸

The following terms and phrases are commonly used during investigations involving white-collar crime.

ATM Fraud (a.k.a. *Credit Card/ATM Fraud*) The unlawful use of a credit (or debit) card or automatic teller machine for fraudulent purposes.

Bribery The offering, giving, receiving, or soliciting of any thing of value (i.e., a bribe, gratuity, or kickback) to sway the judgment or action of a person in a position of trust or influence.

Check Fraud The forgery, alteration, counterfeiting, or knowing issuance of a check on an account that has been closed or has insufficient funds to cover the amount for which the check was written.

¹⁵ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. P 1.

¹⁶ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. P 15.

¹⁷ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. P 1.

¹⁸ Definitions from two sources: (1) the National White Collar Crime Center and (2) an article titled *The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data*. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

<i>Computer Crime</i>	<p>(“True” Computer Crime: Computer as the Target) In the broadest sense, computer crime is a violation of law involving a computer. This broad category of crime is often discussed in terms of two subcategories: “true” computer crime and computer-related crime.</p> <p>“True” computer crime refers to those crimes that target the content of computer operating systems, programs, or networks (hereinafter referred to as “computer systems”) and typically involve one or more of the following:</p> <ul style="list-style-type: none"> • Accessing computer systems without permission (unauthorized access) • Damaging computer systems (sabotage) • Acquiring information stored on computer systems – without permission (theft of data) • Acquiring services from computer systems – without permission (theft of services)
<i>Computer Crime</i>	<p>(Computer as the Instrumentality of the Crime) Computers can be utilized as an instrument or tool to facilitate criminal activity. As defined by the U.S. General Accounting Office, Office of Special Investigations, computers can be “used as tools to commit traditional offenses.” This means that the functions specific to computers, such as software programs and Internet capabilities, can be manipulated to conduct criminal activity.</p>
<i>Counterfeiting</i>	<p>(a.k.a. <i>Counterfeiting/Forgery</i>)The altering, copying, or imitation of something, without authority or right, with the intent to deceive or defraud by passing the copy of thing altered or imitated as that which is original or genuine; or the selling, buying, or possession of an altered, copied, or imitated thing with the intent to deceive or defraud. The altering, copying, or imitation of something, without authority or right, with the intent to deceive or defraud by passing the copy of thing altered or imitated as that which is original or genuine; or the selling, buying, or possession of an altered, copied, or imitated thing with the intent to deceive or defraud.</p>
<i>Credit card fraud</i>	<p>The unauthorized use of a credit card with the purpose of obtaining anything of value with the intent to defraud.</p>
<i>Cyberstalking</i>	<p>There is no universally accepted definition of cyberstalking, yet the term tends to refer to one individual harassing another individual on the Internet using various modes of transmission such as electronic mail, chat rooms, newsgroups, mail exploders, and the World Wide Web. Cyberstalkers can also obtain personal information about their victims (e.g., home address, phone</p>

number) from the Internet and utilize this information to meet their victims in person.

Disaster fraud

Defined as an activity with the purpose to defraud individuals or the government after a natural or man-made catastrophe. Some common examples include unscrupulous operators who persuade disaster fraud victims to claim more damages than actually occurred, contractors who collect money to repair damaged property but never complete the work, and homeowners who increase damage estimates for personal gain.

Embezzlement

(a.k.a. *Embezzlement/Employee Theft*) The Federal Bureau of Investigation (FBI) defines embezzlement as the “misappropriation or misapplication of money or property entrusted to one’s care, custody, or control.” What distinguishes embezzlement from other types of theft is the violation of financial trust between the owner of the money or property and the offender. Embezzlement laws first emerged in England as a response to the inadequacies of larceny statutes that required that property be taken from another’s possession.

Environmental

Environmental violations are those acts or omissions that violate federal, state, or local environmental standards by endangering human health and the environment.

False Pretenses

(a.k.a. *False Pretenses/Swindle/Confidence Game*) The intentional misrepresentation of existing fact or condition, or the use of some other deceptive scheme or device, to obtain money, goods, or other things of value.

Fraud Offenses

The intentional perversion of the truth for the purpose of inducing another person or other entity in reliance upon it to part with some thing of value or to surrender a legal right.

Health care fraud

Intentional deception or misrepresentation, knowing that the misrepresentation can result in some unauthorized medical payment or benefit to the individual, or the entity, or to another party.

Identity theft

The Identity Theft and Assumption Deterrence Act of 1998 (amending 18 U.S.C. § 1028) made it a federal crime when anyone “knowingly transfers or uses without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under an applicable State or local law.”

<i>Impersonation</i>	Falsely representing one's identity or position, and acting in the character or position thus unlawfully assumed, to deceive others and thereby gain a profit or advantage, enjoy some right or privilege, or subject another person or entity to an expense, charge, or liability which would not have otherwise been incurred.
<i>Insurance fraud</i>	Making an insurance claim or increasing the amount of a claim by deceiving or misrepresenting the nature or value of the loss. ¹ It is a form of theft by deception.
<i>Internet fraud</i>	Any type of fraud scheme that uses one or more components of the Internet, such as chat rooms, e-mail, message boards, or Web sites, to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected to the scheme.
<i>Internet Gambling</i>	Gambling occurs when an individual plays a game for something of value, such as money or property, or bets on an uncertain outcome. The Internet provides easy, worldwide access for gaming venues and gamblers. Regulatory and/or criminal violations occur when Internet gambling is conducted from or to a location that prohibits or regulates gambling activities, or when gambling is a guise for criminal activity, such as money laundering or fraud.
<i>Money Laundering</i>	Traditionally understood to be the practice of filtering "dirty" money, or ill-gotten gains, through a series of transactions until the funds are "clean," or appear to be proceeds from legal activities. The United States Criminal Code takes a broader stance towards money laundering, and criminalizes knowingly engaging in a broad array of financial transactions that involve money either derived from or meant to promote various illegal activities, or that involve certain elements of deception.
<i>Organized Crime</i>	<p>The term "organized crime" can mean slightly different things to different people. For our purposes, it is enough to say that organized crime is a continuing criminal enterprise that rationally works to profit from illicit activities that are often in great public demand. Its continuing existence is maintained through the use of force, threats, monopoly control, and/or the corruption of public officials.</p> <p>Other quite serviceable, but slightly different, definitions also exist. For example, some would say that organized crime exists when crime groups specialize in enterprise as opposed to predatory crimes, have a durable hierarchical structure, employ systemic</p>

violence and corruption, obtain abnormally high rates of return relative to other criminal organizations, and extend their activities into the legal economy. Others have opted for a broader definition: “Organized crime consists of organizations that have durability, hierarchy and involvement in a multiplicity of criminal activities”.

The United Nations Office on Drugs and Crime defines organized crime as a “structured group of three or more persons existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences in order to obtain, directly or indirectly, a financial or other material benefit” (where a serious crime is a crime that is subject to at least four years imprisonment).

Legally, there is no precise definition of organized crime that is accepted across the United States. The Organized Crime Control Act of 1970 (the preeminent organized crime law in the nation) declined to pin the term down, in favor of criminalizing damaging activities that organized crime groups tended to participate in, particularly racketeering. The statute defines racketeering as “any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or [some controlled substance violations] [or one of several enumerated laws, generally involving fraud, corruption, transportation of stolen or illegal goods or money laundering].” Specifically, the federal law states that “[i]t shall be unlawful for any person who has received any income derived, directly or indirectly, from a pattern of racketeering activity or through collection of an unlawful debt... to use or invest, directly or indirectly, any part of such income, or the proceeds of such income, in acquisition of any interest in, or the establishment or operation of, any enterprise which is engaged in, or the activities of which affect, interstate or foreign commerce.”

Securities Fraud (a.k.a. *Securities/Investment Fraud*) Securities fraud is any manipulation or deception that affects the purchase or sale of a security and usually includes the misrepresentation or omission of material (significant) information. The definition of a security, in general, is an investment instrument from which an investor expects to derive financial benefit through the efforts of others.

Spoofing/Phishing A technique whereby a fraudster pretends to be someone else’s email or web site. This is typically done by copying the web content of a legitimate web site to the fraudster’s newly created fraudulent web site. Phishing refers to the scheme whereby the perpetrators use the spoofed web sites in an attempt to dupe the victim into divulging sensitive information, such as passwords,

credit card and bank account numbers. The victim, usually via email, is provided with a hyperlink that directs him/her to a fraudster's web site. This fraudulent web site's name (Uniform Resource Locator) closely resembles the true name of the legitimate business. The victim arrives at the fraudulent web site and is convinced by the sites content that they are in fact at the company's legitimate web site and are tricked into divulging sensitive personal information. Spoofing and phishing are done to further perpetrate other schemes, including identity theft and auction fraud.

Telemarketing fraud This term generally refers to any scheme to defraud in which the persons carrying out the scheme use the telephone as their primary means of communicating with prospective victims and trying to persuade them to send money to the scheme. This may include any plans, programs, mail outs, solicitations, or campaigns to entice the purchase of goods, services, or charitable contributions through false representation; fraudulent schemes in which telemarketing is an integral component of the marketing effort including Internet marketing, offers over the telephone, infomercials, and targeted mailings; and using one or more telephone lines or any other telecom medium for false representation.

Welfare Fraud The use of deceitful statements, practices, or devices to unlawfully obtain welfare benefits.

Wire Fraud The use of an electric or electronic communications facility to intentionally transmit a false and/or deceptive message in furtherance of a fraudulent activity.

How Identity Theft Occurs¹⁹

As a reminder, this paper will concentrate on Identity Theft & Fraud as the primary nexus between and across the spectrum of *White Collar Criminal Activity*. For that purpose we must set forth how criminals get and use victims' personal information.

How identity thieves get a victim's personal information:

- They steal wallets and purses containing identification and credit and bank cards.
- They steal mail, including bank and credit card statements, pre-approved credit offers, new checks, and tax information.

¹⁹ ID THEFT: When Bad Things happen to Your Good Name. Federal Trade Commission. September 2002. Pps. 3-4.

- They complete a change of address form to divert mail to another location.
- They rummage through trash for personal data in a practice known as “dumpster diving”.
- They fraudulently obtain credit reports by posing as a landlord, employer or someone else who may have a legitimate need for, and legal right to, the information.
- They find personal information in someone’s home.
- They use personal information people share on the Internet.
- They scam people, often through email, by posing as legitimate companies or government agencies people do business with.
- They get information from the workplace in a practice known as “business record theft” by: stealing customer files out of offices, stealing employee files, stealing or removing patient or student files; bribing an employee who has access to personal files; or by hacking into electronic files.

How identity thieves use a victim’s personal information:

- They call credit card companies, and, pretending to be the other person, ask to change the mailing address on the credit card account. The imposter then runs up charges on the account. Because the bills are being sent to the new address, it may take some time before the victim realizes there’s a problem.
- They open a new credit card account, using the victim’s name, date of birth and SSN. When they use the credit card and don’t pay the bills, the delinquent account is reported on the victim’s credit report.
- They establish phone or wireless service in the victim’s name.
- They open a bank account in the victim’s name and write bad checks on that account.
- They file for bankruptcy under the victim’s name to avoid paying debts they’ve incurred under that name, or to avoid eviction.
- They counterfeit checks or debit cards, and drain the victim’s bank account.
- They buy cars by taking out auto loans in the victim’s name.
- They give the victim’s name to the police during an arrest. If they’re released from police custody, but don’t show up for their court date, an arrest warrant is issued for the victim.

White Collar Crime in The United States

Under the traditional Summary Reporting System, there is a limited amount of information available on white-collar crime. The white-collar offenses that are measured are fraud, forgery/counterfeiting, embezzlement, and similar other offenses. Because white-collar crimes are not Index crimes, the only information available on these offenses is arrest information, which includes age, sex, and race of the arrestee. Additionally, the all other offenses arrest category is very limited in its ability to measure the white-collar offenses included in its counts. This is due to the inability to differentiate the white-collar offenses from the others that also fall in this category. Based upon the most recently published data from the FBI, the arrest rates for the offenses of embezzlement, fraud, and forgery/counterfeiting are much lower than the arrest rates for property crime¹ or for total crimes in general.²⁰

In addition to the different NIBRS offenses, using additional data elements can further define and describe white-collar crime. Even though there is a total of 53 data elements divided into six segments in NIBRS, not all of them will apply to white-collar crimes. Many data elements are applicable only to crimes against persons, while white-collar offenses are primarily crimes against property. The four Group A offenses could potentially have all six segments represented in their data elements, but there is only a limited amount of information available on the Group B offenses. Only arrestee information is collected on Group B offenses, which will include many of the corporate offenses like tax law violations, health and safety violations, environmental law violations, etc.²¹

Four data elements of particular interest for measuring white-collar crime are *offender(s) suspected of using . . . , location type, property description, and type of victim*. High tech crime is well represented by the data element offender is suspected of using . . . with computer as one of the possible choices. Offenses like fraud can be further delineated by the type of victim (e.g., government agency, financial institution, individual), property description, or location type.²²

In 1960, a popular magazine reported that by pocketing cash, jiggering books, stealing merchandise, and a score of other similar practices, employees that year would steal more than \$1 billion—more than twice the amount stolen by all the nation's professional thieves.²³ Currently (2006), according to an article in Time reporting information from the nonprofit National White Collar Crime Center, \$40 billion is lost every year to

²⁰ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

²¹ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

²² The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

²³ Time Magazine. Monday, March 7, 1960.

investor swindles, which is just one section of white collar criminal activity.²⁴ Forty-six years ago, in 1960, white collar crime was almost all defined as being perpetrated by corporate personnel. Not so in the 21st century. Now “outsiders” can easily bilk millions of dollars from a single company.

In 1997 through 1999, white-collar crime accounted for approximately 3.8 percent of the incidents reported to the FBI. The majority of those offenses are frauds and counterfeiting/forgery. Additionally, the Group B offense of bad checks accounted for approximately 4 percent of the arrests during 1997-1999.²⁵

Some of the smartest scam artists target groups united by religion, race or ethnic origin. From 1998 to 2001, at least 80,000 people lost \$2 billion in religious-investor frauds, according to the North American Securities Administrators Association, a group representing state regulators. In fact, most of the eight major frauds one investigator helped uncover in the past year have involved hustlers trying to sell investments to church groups.²⁶

According to Fortune Magazine, as prevalent as such fraud (and stupidity) is in the real world, it can't compare with what happens online. A January 2002 GartnerG2 analyst's report that was cited in the article pegged Internet transaction fraud at a rate 12 times higher than the in-store variety.²⁷

In a recent study that was mentioned in a popular magazine, the Federal Trade Commission estimated that **more than one in 10 Americans had lost money in a scam the previous year**. The majority of victims are between the ages of 25 and 44, according to the FTC; the next biggest group is baby boomers.²⁸ The scams of old involved various and sundry get-rich-quick schemes that seemed to primarily target the lower rungs of the intellectual ladder: print ads promising thousands of dollars a week working from home; postcards declaring that one has won some lottery; Nigerian email frauds; advance fee for loan frauds, etc. In the past, immature and inexperienced people often fell prey to these tactics, looking for some quick easy money.

And what about so-called “savvy people”, the “smart, blue-blooded, movers and shakers” of the business world? How do those people manage to spot and avoid scammers, thereby hanging on to more of their wealth than the average commoner? Money Magazine reported on these folks' ability to avoid being scammed. The long and short of it is exactly opposite of what one would expect: In a study that was performed by the National Association of Securities Dealers (NASD) these people are actually *more* likely

²⁴ Scambuster, Inc. At Time.com: <http://www.time.com/time/magazine/article/0,9171,1019853-2,00.html>

²⁵ The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data. Cynthia Barnett. U.S. Department of Justice. Federal Bureau of Investigation. Criminal Justice Information Services (CJIS) Division

²⁶ Scambuster, Inc. At Time.com: <http://www.time.com/time/magazine/article/0,9171,1019853-2,00.html>

²⁷ Fortune Magazine. Article written by David Lidsky. May 1, 2002

²⁸ Money Magazine. Hello, Sucker. Article written by Donna Rosato. November 2006. Page 112.

than others to fall for investment scams. The article warns against stereotyping victims of scams as “lonely old widows or wide-eyed naifs”.²⁹

Because of education - and warnings that have been reported (and repeated) millions of times - the public has become aware of the most popular schemes therefore the effectiveness of those schemes has diminished for the perpetrator. Never-the-less, all schemes seem to “evolve” to something new and effective. Currently, according to regulators, Affinity fraud, as regulators call it, is among the most effective scams going and the hardest to prevent. Typically the con artist infiltrates a social group like a church or professional club, and then persuades his new friends to enroll in his scheme. The members of that inner circle become an unwitting sales network, spreading word to family and friends.

Such frauds are depressingly common. Last year seven NFL players were allegedly cheated out of \$20 million by International Management Associates, a hedge fund promising 30% annual returns. The fund's manager, (the alleged perp), had worked his way into the players' professional network - he'd even been vetted by the NFL Players Association's Registered Financial Advisors program. A Harvard-educated smooth talker who owned three sports cars and lived in a million-dollar home, [the alleged perp] socialized with players at his hospitality suite at football games and convinced them to invest. A former Philadelphia Eagle player turned over millions of dollars to be invested - and realized it was gone only when the fellow was arrested in May for embezzlement.³⁰

Human psychology makes people vulnerable. Fraud experts and psychologists (and, unfortunately, con artists) have long known that people are not nearly as good at detecting liars as they think. And however much **people** may think themselves as having exceptional “powers of reason”, they **are** in fact **wired to make critical money decisions emotionally**, and with biases that they may not recognize. One way or another, **every financial scam exploits that fact**. The sooner one can recognize the chinks in their mental armor, the better.

Note the following statistics:³¹

- In 2005, the average loss reported by scam victims was \$2,412.
- In 2005, \$682 million was reportedly lost by fraud victims nationally.
- In 2005, 431,118 complaints of fraud were reported to the FTC, an all time high.
- In 2004, an estimated 25 million adults were scammed.

Compared to the estimated frequency of white-collar crime, police investigations, custodial arrests and judicial prosecutions are startlingly low. Street cops and investigators do not generally have the resources to follow up at great lengths at the local level on these types of crimes and the Feds only get involved when the crime(s) reach a

²⁹ Money Magazine. Hello Sucker. Article written by Donna Rosato. November 2006. Page 112.

³⁰ Money Magazine. Hello Sucker. Article written by Donna Rosato. November 2006. Page 112.

³¹ Money Magazine. Hello Sucker. Article written by Donna Rosato. November 2006. Page 112.

certain level, therefore the scams grow to affect a great number of people and involve a tremendous amount of money before being addressed.

The below table lists the demoralizing low number of arrests (compared to actual crimes) nationally for specific crimes as reported by the National White Collar Crime Center. The figures were gleaned from Uniform Crime Reports for 2004.

<u>Crime</u>	<u>Arrests</u>
Forgery/Counterfeiting	86,122
Embezzlement	12,616
Fraud	199,974

A recent survey commissioned by the Federal Trade Commission (FTC) estimated the number of consumer victims of identity theft over the year prior to the survey (which was completed in May 2003) at 4.6 percent of the population of U.S. consumers over the age of 18 (9.91 million individuals) with losses totaling \$52.6 billion (47.6 billion to businesses and \$5 billion to individual victims). However, over half of these victims experienced only the take-over of existing credit cards (5.17 million consumers) which is generally not considered identity theft. New account frauds, more generally considered to be identity theft, were estimated to have victimized 3.23 million consumers and to have resulted in losses of \$36.7 billion (\$32.9 billion to businesses and financial institutions and \$3.8 billion to individuals). Recent research replicating this study for a subsequent twelve-month period obtained similar numbers.³²

Because Identity Theft case data was not provided to the F.B.I. prior to June 2003, an overall statistical analysis will be spotty at best. At the close of Fiscal Year 2004, the FBI had 1,574 pending investigations involving identity theft activity. These cases covered a broad range of investigative classifications.³³

In addition to the F.B.I.'s statistical measurements, another great source of information is the Internet Crime Complaint Center (a.k.a. "IC3"). In December 2003, the Internet Fraud Complaint Center (IFCC) was renamed the Internet Crime Complaint Center (IC3) to better reflect the broad character of such criminal matters having a cyber (Internet) nexus. The 2005 Internet Crime Report is the fifth annual compilation of information on complaints received and referred by the IC3 to law enforcement or regulatory agencies for appropriate action. From January 1, 2005 – December 31, 2005, the IC3 website received 231,493 complaint submissions. This is an 11.6% increase over 2004 when 207,449 complaints were received. These filings were composed of fraudulent and non-fraudulent complaints primarily related to the Internet.³⁴

From the calendar year 2005³⁵ submissions, IC3 referred 97,076 complaints of crime to federal, state, and local law enforcement agencies around the country for further

³² Financial Crimes Report to the Public. U.S.D.O.J. Federal Bureau of Investigation. (Publication)

³³ Financial Crimes Report to the Public. U.S.D.O.J. Federal Bureau of Investigation. (Publication)

³⁴ IC3 2005 Internet Crime Report. Page 2.

³⁵ Calendar Year 2005 is the latest year for which data is available.

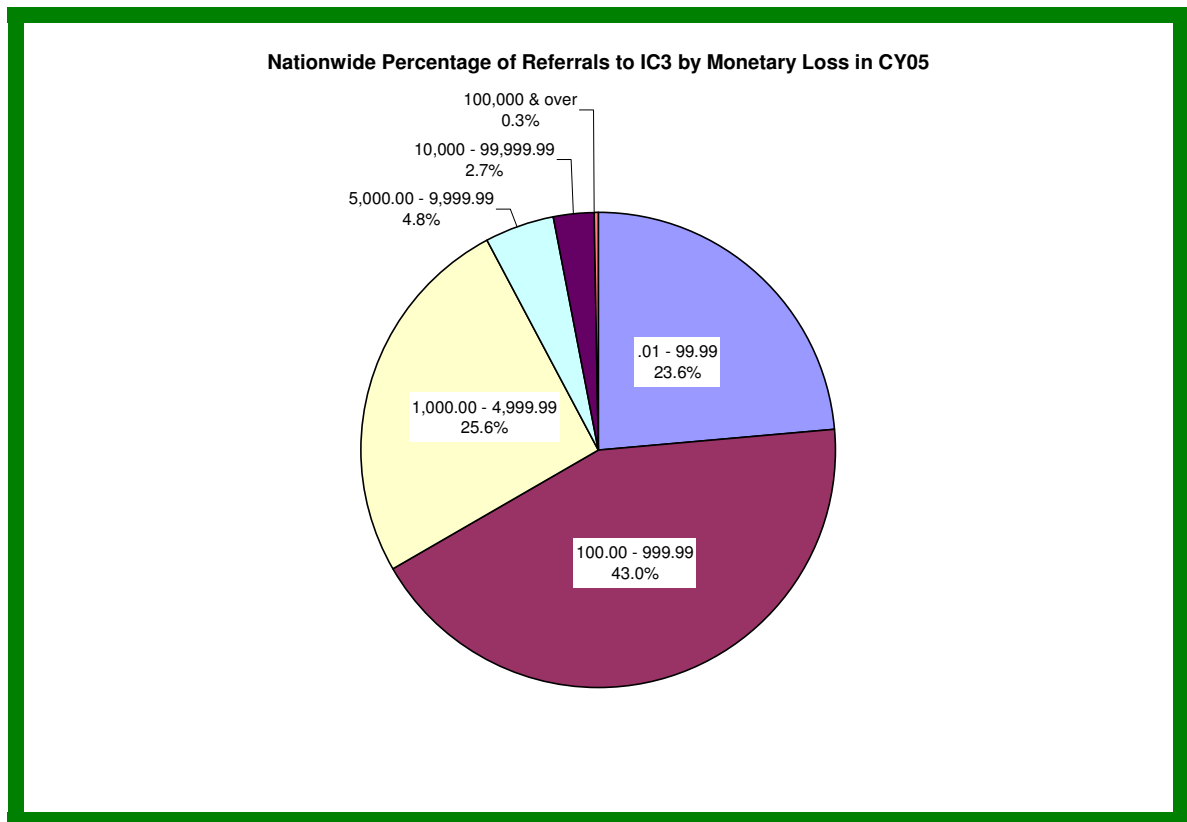
consideration. The vast majority of cases was fraudulent in nature and involved a financial loss on the part of the complainant. The total dollar loss from all referred cases of fraud was \$183.12 million with a median dollar loss of \$424.00 per complaint. This is up from \$68 million in total reported losses in 2004. Other significant findings related to an analysis of referrals include:³⁶

- Internet auction fraud was by far the most reported offense, comprising 62.7% of referred complaints. Non-delivered merchandise and/or payment accounted for 15.7% of complaints. Credit/debit card fraud made up 6.8% of complaints. Check fraud, investment fraud, computer fraud, and confidence fraud round out the top seven categories of complaints referred to law enforcement during the year.
- Of those individuals who reported a dollar loss, the highest median losses were found among Nigerian letter fraud (\$5,000), check fraud (\$3,800), and other confidence fraud (\$2,025) complainants.
- Among perpetrators, nearly 75.4% were male and half resided in one of the following states: California, New York, Florida, Texas, Illinois, Pennsylvania and Ohio. The majority of reported perpetrators were from the United States. However, a significant number of perpetrators were also located in Nigeria, United Kingdom, Canada, Italy, and China.
- Among complainants, 64.0% were male, nearly half were between the ages of 30 and 50 (average age 40.2) and one-third resided in one of the four most populated states: California, Florida, Texas, and New York. While most were from the United States, IC3 received a number of complaints from Canada, Australia, Great Britain, Germany, and Japan.
- Males lost more money than females (ratio of \$1.86 dollars lost per male to every \$1.00 dollar lost per female). This may be a function of both online purchasing differences by gender and the type of fraudulent schemes by which the individuals were victimized.
- Electronic mail (e-mail) and web pages were the two primary mechanisms by which the fraudulent contact took place. In all, 73.2% of complainants reported that they had e-mail contact with the perpetrator and 16.5% had contact through a web page.
- Recent high activity scams seen by IC3 include Super Bowl Tickets scams, phishing attempts associated with spoofed sites, re-shipping, eBay account takeovers, natural disaster fraud, and international lottery scams.

³⁶ IC3 2005 Internet Crime Report. Page 3.

The total dollar loss from all (IC3) referred cases of fraud in 2005 was \$183.12 million. That loss was significantly greater than 2004 which reported a total loss of \$68.14 million; however, this was a direct result of a number of cases in 2005 that reported losses in the millions of dollars. Of those complaints with a reported monetary loss, the mean dollar loss was \$2,202.23 and the median was \$424.00. Twenty four percent (23.6%) of these complaints involved losses of less than \$100.00, and (43.0%) reported a loss between \$100.00 and \$1,000.00. In other words, two-thirds of these cases involved a monetary loss of less than \$1,000.00. A third of the complainants reported high dollar losses, with 25.6% indicating a loss between \$1,000.00 and \$5,000.00 and only 7.8% indicating a loss greater than \$5,000.00. The highest dollar loss per incident was reported by Nigerian Letter Fraud (median loss of \$5,000.00). Check fraud victims, with a median loss of \$3,800.00 and confidence fraud (median loss of \$2,025.00) were other high dollar loss categories. The lowest dollar loss was associated with computer fraud (median loss of \$216.56) and auction fraud (median loss of \$385.00) offenses.

The following pie chart depicts the relative difference in the percent of complaints by monetary loss reported to the IC3 in calendar year 2005.



White Collar Crime in South Carolina

South Carolinians as Perpetrator Statistics Within the United States³⁷

According to the National White Collar Crime Center's Internet Crime Complaint Center (IC3) **in calendar year 2004, per 100,000 population, South Carolina ranked 34th highest at 11.20 while ranking 27th on total number of perpetrators identified as residing in South Carolina.** In calendar year 2005, per 100,000 population, South Carolina ranked 44th highest at 8.60 while ranking 28th on total number of perpetrators identified as residing in South Carolina. This total accounts for 0.9% of all complaints where the perpetrator was identified.

South Carolinians as Complainant Statistics Within the United States³⁸

According to the National White Collar Crime Center's Internet Crime Complaint Center (IC3) in calendar year 2004, Per 100,000 population, South Carolina ranked 27th highest at 28.30 while also ranking 25th on total number of complainants identified as residing in South Carolina. **In calendar year 2005, per 100,000 population, South Carolina South Carolina ranked 4th highest at 80.16 while also ranking 18th in total number of complainants identified as residing in South Carolina.**

Complainant – Perpetrator Dynamics: Contact Method

In calendar year 2004, the number of South Carolinians who perpetrated IC3 type crimes against fellow South Carolinians was 4.2%. This figure was well below the same-state stats for other states and did not come close to the top three in the nation. Florida was number one with 10.8%, California was number two with 10.1% and New York was number three with 8.7%. However, In calendar year 2005, that changed when South Carolina with 8.6% actually had the third highest percentage of any state in the nation with perpetrator and victims to reside in the same state. California was number one with 13.8%, New York was number two with 9.4% and Florida was number 4 with 8.4%.

The method by which victims from South Carolina were contacted was fairly consistent for the two years and they maintained their relative order except that in 2005, chatrooms overtook physical mail and printed material as a more-preferred method of contact. E-mail contact increased significantly in 2005 over its 2004 reported figure.

<u>Complainant - Perpetrator Dynamics: Contact Method</u>		
	<u>2004</u>	<u>2005</u>
E-Mail	57.3%	70.9%
Webpage	27.8%	17.6%
Phone	7.9%	4.5%
Chatrooms	1.6%	2.4%
Physical Mail	2.2%	2.1%
Printed Material	1.8%	1.3%
In Person	1.2%	1.2%
Fax	0.2%	N/L
TOTAL	100.0%	100.0%

³⁷ Statistics from South Carolina's IC3 2004 & 2005 Crime Reports.

³⁸ Statistics from South Carolina's IC3 2004 & 2005 Crime Reports.

White Collar Crime in the City of Anderson, South Carolina

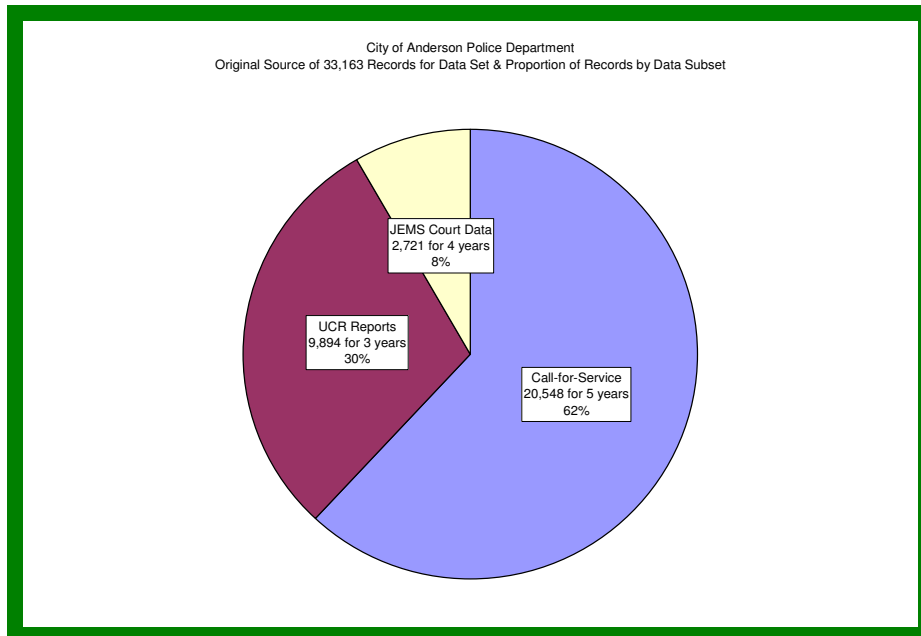
Data source

The following analysis will utilize three types of data. The most general form of data will be the *call-for-service data* which is uploaded from Anderson County Central Dispatch. The second type of data that will be used will be the *Uniform Crime Report (UCR) data* regarding police reports which was uploaded in-house from the Police Central database.³⁹ The most specific type of data will be the *court docket data* from the JEMS software program.⁴⁰ That data will be an actual report of the types of white-collar crimes that were charged in the City of Anderson.

Due to the fact that there are three different types of data, ranging from the very general (calls-for-service) to the very specific (JEMS Court Data), and because the subsets of data are for a different number of years (albeit all years are consecutive and end at the end of fiscal year 2006), in order to get an accurate picture of the data and the relevant level of importance of each subset of data, each subset will be analyzed separately, with separate conclusions drawn from each subset. Finally a summary conclusion will be proffered which will attempt to explain the findings as a whole.

The original source for white collar crime data available from the City of Anderson Police Department Records Division are (1) calls-for-service statistics for 5 years, (2) Court Docket data for 4 years and (3) Uniform Crime Reports for 3 years. For reference the data subsets are detailed in the table and chart that follows.

Data Set for White Collar Crime Stats			
Data Subset	Years of Data	Records	Average per Year
Call-for-Service	5	20,548	4,110
UCR Reports	3	9,894	3,298
JEMS Court Data	4	2,721	680
TOTAL		33,163	



³⁹ The Police Central database is the software program utilized by the City of Anderson Police Department to write, compile, transmit and analyze criminal activity.

⁴⁰ JEMS is an acronym for the Judicial program utilized by the City of Anderson Municipal Court.

**Calls-for-Service⁴¹ Related to
White Collar Criminal Activity in Anderson, South Carolina**

Data for the five fiscal years ending June 30, 2006, was available from the City of Anderson Police Department's call-for-service data banks for the following types of alleged, suspected, or actual criminal activity which is related to white collar crime:

White Collar Crime-Related Calls-for-Service by Fiscal Year						
Call Type	2002	2003	2004	2005	2006	Total
Bad Check	27	21	30	38	18	134
Breach of Trust	127	98	79	96	97	497
Break-In	702	618	650	652	750	3,372
Break-In: Auto	146	98	79	85	74	482
Civil Dispute	836	895	903	1,032	928	4,594
Forgery	212	224	192	217	229	1,074
Larceny	1,283	1,401	1,581	1,569	1,574	7,408
Larceny: Gas Drive Off	292	311	350	230	80	1,263
Larceny: Shoplifting	326	410	250	365	324	1,675
Prostitution	7	3	15	9	7	41
Purse Snatching	5		1		2	8
Total	3,963	4,079	4,130	4,293	4,083	20,548

Bad checks, breach of trusts, forgeries and larcenies are commonly known as white collar crimes. However, there is a correlation between white collar criminal activity and break-ins of houses and vehicles because those places are where checks, credit cards and other items containing personal identifiers are originally stolen. Additionally, civil disputes are almost always the result of a business operator calling the police about someone who has flimflammed them or attempted to rip-off the business-person in some other way. Some civil disputes are private citizens calling for the same purpose.

Of particular importance in the above-referenced statistics is the fact that the bad check numbers are under-reported. Because the department has so many bad checks referred to it on a weekly basis, the policy of the City of Anderson Police Department is to not cut a case number (i.e. we do not open a "call-for-service record") until after a warrant is issued and served. Therefore, the call-for-service records for bad checks listed above generally refer only to instances wherein a person has been apprehended and/or served with a warrant. The above-referenced call-for-service numbers are an under-reporting of the figures and do not accurately reflect the total number of times a bad check has been referred to the City of Anderson Police Department.

Of the 20,548 calls-for-service handled by the City of Anderson Police Department for the last five consecutive fiscal years, 15,445 (75.2%) occurred on business days, Monday through Friday. Of those calls, 10,779 were dispatched between 07:00 and 18:59, indicating a strong correlation between white-collar crime and the portion of the business day that most businesses are open. The 10,779 calls-for-service dispatched to officers of

⁴¹ Call-for-service data originally obtained from Anderson County Central Dispatch.

the City of Anderson Police Department on Monday through Friday between 07:00 & 18:59 represented 52.5% of the total for all white-collar crime calls and 69.8% of all white collar crime dispatched on business days. The next two tables depict by day and by hour of day the number of white-collar related calls-for-service that were dispatched between fiscal year 2002 and 2006.

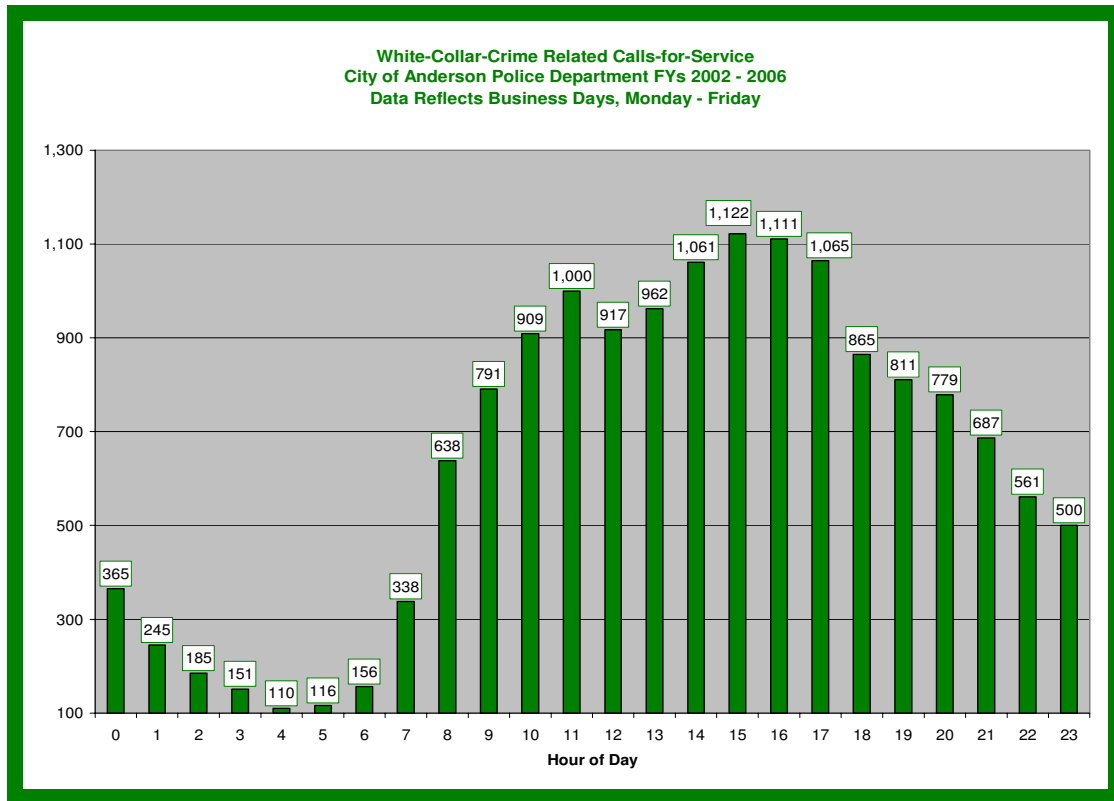
Number of white-collar-crime related calls-for-service dispatched to the City of Anderson Police Department by day of week from FY02 – FY06:

<u>Day of Week</u>	<u>Total</u>	<u>Percent</u>
Sunday	2,126	10.3%
Monday	3,115	15.2%
Tuesday	3,065	14.9%
Wednesday	3,070	14.9%
Thursday	3,011	14.7%
Friday	3,184	15.5%
Saturday	2,977	14.5%
Grand Total	20,548	100.0%

Number of white-collar-crime related calls-for-service dispatched to the City of Anderson Police Department by hour of business day from FY02 – FY06:

New Hour	W/C Crime CFS Dispatched	New Hour	W/C Crime CFS Dispatched
0	365	12	917
1	245	13	962
2	185	14	1,061
3	151	15	1,122
4	110	16	1,111
5	116	17	1,065
6	156	18	865
7	338	19	811
8	638	20	779
9	791	21	687
10	909	22	561
11	1,000	23	500
Grand Total			15,445

The following chart depicts the white-collar-crime related calls-for-service that occurred on business days for the five-year period ending June 30, 2006.



As depicted by the above chart, starting at about 07:00 the calls increase dramatically and climb steadily, in sequence with the business day. As banks and businesses close, the calls begin to decrease. During the hours that businesses are closed, the dispatched calls for white-collar-related-crime is minimal. The fact that the above chart depicts most of the suspected white-collar-related crimes that we have listed as being correlated strongly with the times of day that businesses are open supports our thesis that most if not all of these listed crimes are carried out potentially in support of financial crimes.

Uniform Crime Reports⁴² (UCRs) Related to White Collar Criminal Activity in Anderson, South Carolina

Uniform Crime Reports (UCRs) are the actual written reports of activity – criminal and otherwise – that police officers use to document various types of incidents that occur during the course of business. The incidents listed in this section of the report are “not overlapping”, i.e. they are in addition to each other. Some of the crimes such as *obtaining goods under false pretenses* involve several offense types. The reports are usually written by police officers “on the street”. Electronic data for the three fiscal years ending June 30, 2006, was available from the City of Anderson Police Department’s UCR data banks for the following types of alleged, suspected, or actual criminal activity which is related to white collar crime:

⁴² From Police Central NIBRS/SCIBRS Records Management System, City of Anderson P.D. UCR data reported from fiscal years, 2004, 2005 & 2006.

White Collar Uniform Crime Reports by Fiscal Year				
State Statute	2004	2005	2006	Grand Total
Attempt To Obtain Controlled Substance {44-53-420a}		3	3	6
Attempting To Obtain A Prescription By Fraud {44-53-40}			3	3
Auto Breaking {23f}	10			10
B/E Motor Vehicle {16-13-160}	89	68	88	245
Bank Fraud {34-3-110}	3	5	7	15
Begging/Soliciting Alms {62-13}		3	14	17
Breach Of Trust {16-13-230}	117	138	143	398
Breach Of Trust {26a}	5			5
Computer Crime Act 16-16-20			10	10
Conspiracy 44-53-375			9	9
Counterfeiting {State}	43	34	40	117
Credit Card Fraud {16-14-60}	53	66	70	189
Credit Card Theft {16-14-20}	10	9	22	41
Defrauding Innkeeper {45-1-50}	6		8	14
Defrauding Restaurant {62-170a}		3		3
Failure To Pay Cab Fare {33-37}	20	29	22	71
Failure To Pay Food Bill {62-170}	9		8	17
Failure To Pay For Gasoline {16-13-185}			6	6
Financial Identity Fraud {16-13-510}	18	14	34	66
Forgery {16-13-10}	202	350	401	953
Forgery {250}	18			18
Fraud {26a}	1			1
Fraudulent Application For Id {57-3-950}	3			3
Fraudulent Check {34-11-60a}	734	443	101	1,278
Fraudulent Check 1st Offense {34-11-60b}	6	3		9
Fraudulent Check Over 500 {34-11-60}	6	21	3	30
Frequent House Of Ill Fame {90z}	3			3
Fugitive From Justice {17-9-10}	18	58	68	144
Fugitive From Justice {90z}	3			3
Gambling {62-288a}		11	4	15
Gas Drive Off {State}	19	15	18	52
Giving False Information {16-17-725}	52	127	114	293
Identity Theft 16-13-510			7	7
Impersonating An Officer {16-17-720}	3	3		6
Misrepresentation Of Identity {56-1-510}	10	69	54	133
No Business License {26-44 Cc}	3	17	19	39
Obt Goods Under False Pretense {16-13-240}	24	21	52	97
Obt Goods Under False Pretenses (Check) {34-11-60c}	272	260	80	612
Obtaining Drugs By Fraud {44-53-390}		21	24	45
Obtaining Prescription Drugs By Fraud {26a}	3			3
Petty Larceny {16-13-30}	669	778	1,047	2,494
Petty Larceny 3rd & Sub {16-1-57}	4	16	30	50
Pilfering Motor Vehicle {82-13a}	62	50	57	169
Poss False Id {56-1-510a}			3	3
Poss Gambling Devices {62-288}		5	3	8
Possession Of Stolen Property {280}	7			7
Prostitution {16-15-90}		13	16	29
Purse Snatching {16-13-150}	2	2	8	12
Rec/Poss Stolen Goods {16-13-180}	67	144	165	376
Safe Cracking {16-11-390}	2			2
Shoplifting {16-13-110}	377	609	675	1,661
Shoplifting 1st Offense {23c}	25			25
Solicitation For Immoral Purposes {62-252a}		8	6	14
Solicitation For Prostitution {98-1}		6		6
Stolen Prop 3rd & Sub {16-1-57 (1)}		8	10	18
Stop Payment On Check W/Fraud Intent {34-11-80}	3	3		6
Stop Payment On Chk W/Fraud Intent {46-11-80}		3		3
Tampering W/Utility Meter {16-13-385}		10	6	16
Tampering With Food Or Drugs 16-3-75			2	2
Theft Of Electric Current {16-13-380}	4		3	7
Grand Total	2,985	3,446	3,463	9,894

As with crimes listed within the calls-for-services, certain reported crimes are commonly known as white collar crimes. The above-listed summary of white collar activity includes those additional crimes that are not readily recognized as white-collar in nature. The summarized information also contains the crimes that normally give rise to white-collar criminal activity, such as car and house break-ins. Also, as with calls-for-services, the bad check numbers are under-reported, and for the same reasons as the call-for-services. Generally, reports are not written for bad checks unless a warrant is issued and served on an arrested subject. We do not write reports every time we get a bad check reported, turned in or a warrant issued. We get bad checks referred to us so frequently that we only write reports after an arrest is made.

The criminal incidents listed on the above-referenced reports far exceed the per-capita “one in 10” ratio for white-collar criminal victimization in the United States. Based upon a population of 25,563⁴³ the three years incident ratios for 2,985, 3,446 and 3,463 would equate to ratios of 11.7, 13.5 and 13.5 respectively.

There was an average of 2.5 incidents per each of the 3,956 UCR reports taken for the above-referenced crimes. The range for number of incidents per reports was 1 to 24. The mean number of incidents per report was 3. The mode was 3 also with 1,645 reports containing three incidents each.

Number of Incidents per Report	Occurrences
1	854
2	1057
3	1645
4	257
5	48
6	54
7	4
8	16
9	4
10	12
12	1
15	1
16	1
20	1
24	1
Grand Total	3,956

It is interesting to note that the case with 24 incidents had 8 counts of shoplifting listed along with 8 counts of False Pretenses / Swindling / Confidence Game and an additional eight “other” charges.⁴⁴ Of particular interest is the fact that the computer crime incidents involved wire fraud and the conspiracy charges that were written involved narcotics trafficking, thus supporting our theory that financial crimes buttress other illegal activity.

⁴³ U.S. Census estimate for Anderson, South Carolina (2003).

⁴⁴ Case # 05-22200

Counterfeiting & Type of Victim in Anderson, South Carolina

The 117 counterfeiting reports had businesses listed for almost all of the incident locations. With 24 reported incidents, specialty stores topped the list of counterfeiters' preferred victims, followed by convenience stores (19) and banks (13). Three of the counterfeiting incidents at a specialty were at a Mexican tienda. The three reported incidents for government buildings were actually at the DMV, indicating that crooks are getting bold at committing fraud to get a "legal" (government) false ID.

<u>Location Type Where Counterfeiting Reported</u>	<u>Total</u>
Bank/Savings and Loan	13
Bar/Night Club	3
Commercial/Office Building	5
Convenience Store	19
Department/Discount Store	12
Drug Store/Dr. Office/Hospital	5
Government/Public Building	3
Grocery/Supermarket	4
Malls/Shopping Malls	3
Other/Unknown	8
Parking Lot/Garage	1
Residence/Home	5
Restaurant	6
School	3
Service/Gas Station	3
Specialty Store	24
Grand Total	117

The 16 tampering with utility meter reports all occurred at homes, residences and apartments (or condominiums). None were businesses, per se, *unless we consider apartments as a business in this context.*

The 709 incidents that involved **obtaining goods under false pretenses** included virtually all business types and spanned several white-collar crimes. In fact, this type of offense **seems to be a "text-book" example of the type of offense they typifies white-collar criminal activity.** Checks were the most often used "tool" by the perp that obtained goods (or attempted to obtain) by false pretenses. "Obtaining goods..." is the actual state statute that was written as having been the South Carolina state law that was violated. The incidents listed are the federal classification that was listed as being the primary offense type for the crime at the time. These incidents are not "overlapping"; these 709 offense types are all in addition to other offense types listed in other tables.

<u>Offense Types for Obtaining Goods Under False Pretenses</u>	<u>Total</u>
All Other Larceny {23h}	6
Bad Checks {90a}	607
Counterfeiting / Forgery {250}	14
Embezzlement {270}	2
False Pretenses / Swindle / Confidence Game {26a}	70
Fraud {26a}	2
Impersonation {26C}	2
Non-Reportable {90t}	3
Obtaining Goods By False Pretenses {26a}	3
Grand Total	709

The location where the incidents occurred involved primarily businesses:

<u>Location Type for Obtaining Goods Under False Pretenses</u>	<u>Total</u>
Apartments/Condominiums	3
Bank/Savings and Loan	6
Colleges/Universities	3
Commercial/Office Building	3
Convenience Store	178
Department/Discount Store	262
Drug Store/Dr. Office/Hospital	39
Government/Public Building	7
Grocery/Supermarket	24
Highway/Road/Alley	2
Malls/Shopping Malls	27
Other/Unknown	38
Parking Lot/Garage	2
Residence/Home	12
Restaurant	15
Service/Gas Station	6
Specialty Store	82
Grand Total	709

Court Docket⁴⁵ (Prosecution) Data Related to White Collar Criminal Activity in Anderson, South Carolina

Prosecution data for the four fiscal years ending June 30, 2006, was available from the City of Anderson Municipal Court Docket for the following types of criminal activity which is related to white collar crime:

Pivot Table of Court Charges for White Collar Crime by Fiscal Year: 2003 - 2006					
Charge	FY03	FY04	FY05	FY06	Grand Total
Bad Check			8		8
Begging/Soliciting Alms	1		1	5	7
Breach Of Trust	28	23	15	22	88
Computer Crime Act				1	1
Credit Card Fraud	40	7	9	16	72
Credit Card Theft	8	1	8	1	18
Criminal Conspiracy	7			17	24
Embezzlement Of Public Funds		1			1
Failure To Pay Cab Fare	1	7	9	4	21
Failure To Pay For Gasoline	1	2	1		4
Filing False Report	3	2	1	2	8
Forgery	138	214	51	43	446
Fraud: Bank Fraud	3		1	3	7
Fraud: Defrauding Innkeeper	2		1		3
Fraud: Defrauding Restaurant	1		1		2
Fraud: Financial Identity Fraud	1			7	8
Fraud: Housing Fraud		1			1
Fraud: Stop Payment On Check W/Fraud Intent	1		2		3
Fraudulent Check	82	15	110	66	273
Fugitive From Justice	10	15	16	16	57
Gambling		3	1		4
Gambling: Permitting Gambling				1	1
Gambling: Punch Boards			1	1	2
Gambling: Poss Gambling Devices		1	1		2
Giving False Information	35	36	47	34	152
Misrepresentation Of Identity	5	7	27	20	59
No Business License	4	3	4	8	19
Obtaining Drugs By Fraud	1	1	2	12	16
Obtaining Goods Under False Pretenses	52	22	49	54	177
Perjury			2	1	3
Poss False Id		2			2
Poss Stolen Goods	8	6	8	16	38
Poss Stolen Pistol	1	5	2	7	15
Poss Stolen Property		2	1		3
Possession Of A Vehicle With Vin Plate Removed				1	1
Possession Of Stolen Vehicle	5	15	9	22	51
Provisions Of The International		1			1
Purse Snatching	4			2	6
Rec/Poss Stolen Goods	33	28	33	33	127
Shoplifting	267	192	216	193	868
Shoplifting 3rd & Sub	7	15	19	11	52
Solicitation For Immoral Purposes	2		4	3	9
Solicitation For Prostitution	1	1	1		3
Stolen Prop 3rd & Sub			7	2	9
Tampering W/Utility Meter			3		3
Unlawful Sale Of Beer	1		3	2	6
Unlawful Sale Rolling Papers			2		2
Unsafe Structure	11				11
Use Of Vehicle W/O Owners Consent	1	9	12	4	26
Use Of Water Without Permit		1			1
Grand Total	765	638	688	630	2721

⁴⁵ From JEMS Judicial System Database.

It is interesting to note that only 385 fraud charges were prosecuted by the City of Anderson Police Department between fiscal years 2003 and 2006.

Charge (From Court Docket)	FY03	FY04	FY05	FY06	Grand Total
Credit Card Fraud	40	7	9	16	72
Fraud: Bank Fraud	3		1	3	7
Fraud: Defrauding Innkeeper	2		1		3
Fraud: Defrauding Restaurant	1		1		2
Fraud: Financial Identity Fraud	1			7	8
Fraud: Housing Fraud		1			1
Fraud: Stop Payment On Check W/Fraud Intent	1		2		3
Fraudulent Check	82	15	110	66	273
Obtaining Drugs By Fraud	<u>1</u>	<u>1</u>	<u>2</u>	<u>12</u>	<u>16</u>
Grand Total	131	24	126	104	<u>385</u>

During the same years that the above-referenced 385 charges were investigated and prosecuted, at least 5,097 calls-for-service were dispatched to address white-collar criminal activity that the City of Anderson Police Department believes was directly related to the above-referenced types of crimes as follows:

Call-for-Service Type	2003	2004	2005	2006	Grand Total
Bad Check	21	30	38	18	107
Breach of Trust	98	79	96	97	370
Civil Dispute	895	903	1,032	928	3,758
Forgery	224	192	217	229	862
Grand Total	1,238	1,204	1,383	1,272	<u>5,097</u>

During the last four consecutive fiscal years, roughly 7%⁴⁶ of calls-for-service for potentially fraudulent activity resulted in an actual criminal charge. Interesting, between 2004 and 2006, despite the fact that an estimated 3,859 individual calls-for-service were dispatched for the above-referenced typed of fraud, only 1,668 actual incidents were documented on UCR reports, indicating that officers may be misinterpreting fraudulent calls as a purely civil matter. As indicated by the court docket data, only 254 charges (roughly 6% of dispatched calls) were prosecuted in that three-year period.

The following incidents were documented in the UCR reports and apply directly to the fraudulent call-for-service and court docket charge types.

State Statute (From UCR Report)	2004	2005	2006	Grand Total
ATTEMPTING TO OBTAIN A PRESCRIPTION BY FRAUD {44-53-40}			3	3
BANK FRAUD {34-3-110}	3	5	7	15
CREDIT CARD FRAUD {16-14-60}	53	66	70	189
DEFRAUDING INNKEEPER {45-1-50}	6		8	14
DEFRAUDING RESTURANT {62-170A}		3		3
FINANCIAL IDENTITY FRAUD {16-13-510}	18	14	34	66
FRAUD {26A}	1			1
FRAUDULENT APPLICATION FOR ID {57-3-950}	3			3
FRAUDULENT CHECK {34-11-60A}	734	443	101	1,278
FRAUDULENT CHECK 1ST OFFENSE {34-11-60B}	6	3		9
FRAUDULENT CHECK OVER 500 {34-11-60}	6	21	3	30
OBTAINING DRUGS BY FRAUD {44-53-390}		21	24	45
OBTAINING PRESCRIPTION DRUGS BY FRAUD {26A}	3			3
STOP PAYMENT ON CHECK W/FRAUD INTENT {34-11-80}	3	3		6
STOP PAYMENT ON CHK W/FRAUD INTENT {46-11-80}		3		3
Grand Total	836	582	250	<u>1668</u>

⁴⁶ 385 out of 5,097.

II. Existing Efforts and Current Resources

According to the City of Anderson Police Department, white collar criminal activity as we presently know it consists of the following crimes:

1. Forgery
2. Bank Fraud
3. Credit Card Fraud
4. Credit Card Theft
5. Financial Identity Theft
6. Breach Of Trust (Employee/Employer Relationship)
7. Computer Crimes Act

At this time the department has 112 cases pending for either an arrest or a final disposition for prosecution.

When information was solicited from investigators about white collar crime in Anderson, a summary of their views was prepared and summarized as follows. The summary states:

“[They] have come to the realization that every case cannot be worked. White collar criminal activity is the fastest growing crime in America today. It has most definitely out grown the manpower available at this department. At this time there is only one person investigating these types of crimes with the Anderson City Police Department. Some cases have leads, some don't. Some cases just get so old that they are forgotten due to so many new cases coming in. In a lot of these cases, evidence is lost due to the time factor.

“In fact, some cases are not even accounted for by anyone except the one investigator who occasionally gets to work one of them. These cases are generally the more in-depth ones where a lot of man hours have been spent trying to determine the actual jurisdiction of the crime, or even if there has been an actual crime that has taken place. Many of these cases were referred to the City of Anderson Police Department by another agency, or victim from out of state, that called directly into the P.D.

“On a monthly basis the department picks up an envelope from a local department store that contains approx 20 to 60 forged or counterfeit checks and money orders. These documents are turned over to the Investigative Services Division. Again, as suspected by the correlation between calls-for-services, UCR reports and Court Docket charges, reports are not generated on these cases. Some local department stores do not require a report and a lot of these checks are from out of state. Usually with these checks our investigator conducts a cursory review to determine if he may already be working a case on the possible perpetrator. This represents just one business in the city. Although most businesses file some sort of

report, not all do. One thing that can always be counted on is new cases coming in and backing up.

“There are also counterfeit money cases that get reported to Anderson P.D. These cases and evidence are *usually* forwarded to the U.S. Secret Service as they come in.

“Most forgery cases have some kind of monetary loss to them. Some do not have a monetary loss, but we still have a forgery victim. For instance, this occurs when someone obtains a driver’s license in someone else name. The DMV forms have been forged, but no one has lost any money (yet).

“Some white collar crimes that we do work to fruition are closed in as little as half a day, while others may take a month or longer. In most cases, the investigator is usually trying to investigate multiple cases at any one time. Usually 3 to 5 cases at a time.

“Computer crimes are the most time consuming. EBay fraud cases can take up a lot of time and paperwork for just a few hundred-dollar loss.

“There are several types of breach of trust crimes. The only ones we normally investigate are the ones that involve employee and employer relationship. This would be cases wherein an employee steals from a business or someone hires a person to do work and it turns out being some type of scam.

“Credit card fraud cases may include multiple charges on one credit card. Anything fraudulently charged within a six-month period is all included into one warrant. So, where you might have 10 different purchases on the same credit card, only one arrest warrant will be issued. But, all ten purchases are investigated individually.

“The white collar crime investigations take a back seat to providing investigative assistance on other types of cases.”

As suspected from the comparison between calls-for-services, UCR reports and Court Docket charges, information solicited from investigators indicates that some cases are referred to them with no report generated. For instance, when time permits, the one investigator who handles these cases is currently looking into a case sent to him from Wachovia. The case involves multiple forgeries that have an estimated loss to Wachovia in the amount of \$120,000.00. Although not all the loss is in this jurisdiction, some of it is.

With only one investigator to handle the white collar criminal activity in the city of Anderson on a part time basis, and with no special training in this area, the performance is low when compared to the potential. In other words, there are a great number of cases that could potentially be made but the lack of trained personnel who are assigned full time to these types of crimes renders the crimes uninvestigated, unsolved and unprosecuted. The perpetrators are free to continue victimizing innocent people.

III.

Conclusion

In the City of Anderson, between 2004 and 2006 an estimated 3,859 individual calls-for-service were dispatched for suspected cases of fraud, only 1,668 actual incidents were documented on UCR reports and a mere 254 charges were prosecuted in that three-year period. Although Fraud is a major nexus between many different white collar crimes, it is just one component and these performance statistics indicate that a great many cases of white-collar criminal activity are un-investigated (or “under-investigated”).

Anderson, South Carolina has a higher per capita rate of white-collar crime than the average for the United States and the state of South Carolina. Exasperating this finding is the fact that investigators within the City of Anderson Police Department do not have time to investigate white-collar crime due to the fact of an excessive workload of violent & property crime. Unfortunately, according to the research presented in this paper, the types of people who seem to commit many property crimes - and possibly many violent crimes - are probably involved in additional types of crimes related to white-collar activity, either directly or indirectly.

The severity of white-collar crime in the United States, South Carolina and Anderson City is rising. The number of crimes is increasing and the dollar losses are going up. The compound result of these two factors is a geometric increase in victimization. Contemporary crooks are more sophisticated and computer savvy than the ones of previous generations. When financial and identity theft crimes occur, *more people are bilked out of more money, faster* than a decade ago. Statistics indicate that proactive measures must be taken or there will be an annual increase in the number of people who have their lives and finances fouled up because of identity theft and financial crimes. South Carolina is near the top of the list of states wherein people are victimized by white collar criminals who reside in the same state and Anderson City contributes disproportionately to the numbers for white collar criminal activity.

Based upon our research of white-collar crime, which demonstrates a significant amount of un-followed-up investigations into financial and identity theft crimes in Anderson City, we estimate that a substantial increase in white-collar prosecutions can be realized if we were to have investigators who are dedicated solely to investigating white-collar crime. Work-study analysis of the City of Anderson Police Department Detective Unit indicates that when functioning at or near 100% efficiency, individual investigators can build and prosecute 63 - 96 cases per year⁴⁷ against *individual* perpetrators. Most white collar crooks commit numerous crimes each; therefore for each 63-96 perps prosecuted, several times that amount of cases could be cleared.

To go after and prosecute *all* potential white-collar crime cases would require several additional investigators. The City of Anderson currently assigns these cases to investigators based upon availability and cannot afford to increase the number of

⁴⁷ Analysis bases upon FY 2000 and FY 2001. Actual number within range depends upon type of crime and whether or not the crime is tried in City Court or General Sessions Court.

investigators with existing municipal funding. Police Department funding through the general revenue is projected to stay at its current level for at least several more years thus precluding the department from adding additional personnel without outside funding. **Funding for a White-Collar Crime Investigative Unit would result in a higher clearance rate and increased number of prosecutions for white-collar crime cases starting in fiscal year 2008 and would reduce future occurrences of white collar crime in Anderson City,** as the investigator will be removing bad role-models from society, taking embezzlers, swindlers and identity thieves off the streets and following up on and prosecuting individuals who conspire with these types of characters to commit financial crimes.

