FRAUD: THE CHARACTERISTIC CRIME OF THE TWENTY-FIRST CENTURY

*Jay S. Albanese**

In the same way that larceny characterized much of twentieth century, fraud will likely characterize the twenty-first century. Larceny remains the most common of all serious crimes, but fraud may overtake larceny as the crime of choice in the future, because of changes in our ownership, storage, and movement of property. Fraud involves purposely obtaining the property of another through deception, and its popularity as a crime of choice is growing. Entrusting property to the custody of others, storing property at remote locations, and electronic movement of property are shown to be major changes in the way we treat property and increase opportunities for theft. The connection between fraud and many of the serious crimes of the twenty-first century are shown in the facts of recent cases. The motivation of theft behind many frauds is also shown to be used to fund larger criminal objectives, such as illegal immigration and terrorism.

In the same way that larceny characterized much of twentieth century, fraud will likely characterize the twenty-first century. Larceny, defined as taking property of another with intent to deprive the owner, remained at high levels throughout the 1900s, and is the most common of all crimes. In the United States, for example, larcenies reported to police rose from 4.3 million during the 1970s to 7.1 million by 2002 (Federal Bureau of Investigation, 2004). Victimization surveys (including both crimes reported to police as well as those unreported) revealed stable, but much higher levels of larcenies at approximately 14 million incidents per year, far surpassing the volume and rate per 1,000 population of any other serious crime (Bastian et al., 2004).

Fraud is defined as purposely obtaining the property of another through deception, and its popularity as a crime of choice is growing. The connection between fraud and many of the serious crimes of the twenty-first century can be seen from the facts of recent cases.

A two-year investigation into the illegal practices of Indonesian immigration brokers resulted in an indictment alleging that the owners, employees and associates of these brokerages knowingly defrauded the government for several years. Thousands of Indonesian immigrants living throughout the United States were aided in fraudulently applying for a wide variety of government benefits through alien labor certification, Virginia driver's licenses and identification cards, United States passports, and Social Security cards. The investigation revealed that fraudulent asylum applications for Indonesian clients were prepared in return for a fee of $2,000 or more. These applications typically contained false claims that the applicant had been raped, sexually assaulted, beaten, or robbed by Muslims in Indonesia on account of the applicant's Chinese ethnicity or adherence to Christianity. The defendants often supported these claims with counterfeit Indonesian documents, such as birth certificates, baptismal certificates and police reports. The investigation also revealed that these same defendants coached their clients to exploit the perceived sympathies of the asylum officers and immigration judges assigned to consider the applications. In addition, Indonesian clients were routinely aided to obtain Virginia Department of Motor Vehicles (DMV) driver's licenses, learner's permits and identification cards by fraud (*U.S. Fed News*, 2004).

The U.S. government brought fraud accusations against two Moroccan defendants originally charged in the first major terrorism trial since the September 11, 2001 attacks. The superseding indictment alleged that they devised a scheme to defraud Titan Insurance Company by filing false claims. The pair claimed they were injured in a July 5, 2001 auto accident and submitted fraudulent claims for lost wages, physical therapy, and household services. An alleged Detroit terror cell—which the government said included the four men—came to light six days after the World Trade Center attack when federal agents raided an apartment and found false IDs and other materials that the government claimed were blueprints for terror attacks (*Associated Press*, 2004).

These cases connect the simple motivation of theft that motivates many frauds with larger attempts at illegal immigration, false identity documents, terrorism, and other crimes, illustrating that fraud is often used to fund other criminal objectives. Why is fraud becoming a crime of choice among both thieves and those with larger criminal objectives?

Ownership and Storage

There has been a fundamental shift in the method by which property is owned. This shift has occurred for reasons of changes in technology, communications, and globalization. For much of the twentieth century personal and business cash and property was kept physically on the premises, in safety deposit boxes, or in local banks. In every case, the owner had quick, direct physical access to the property at all times. This situation has changed. In contemporary society credit and debit transactions are overtaking cash transactions in volume, and personal property is increasingly leased or borrowed rather than owned. Therefore, fewer people are holding cash or valuables on their person or in their homes, making larceny less attractive as a crime.

Efforts to conceal ownership sometimes occur either to perpetrate a fraud or to conceal other kinds of criminal activity. A former employee of a used automobile dealership pleaded guilty to taking part in a complex money-laundering scheme intended to exchange drug sale proceeds for luxury vehicles. Invoices, financing, and other documents were forged or altered to disguise customer identities and the true nature of financial transactions. The dealership was suspected of selling vehicles to known narcotics dealers and filing false forms in order to disguise the true purchaser of the vehicles (Jardini, 2004). This case illustrates how fraud can be used to disguise not only the source of funds needed to purchase property, but also conceal the actual owner of the property. Similar kinds of frauds have been used to conceal the identities of victims of trafficking in human beings, the smuggling of natural resources, and other kinds of theft, concealment, and illegal transport (United Nations Interregional Crime and Justice Research Institute, 2004; Warchol, 2004; Krebs, 2004).

Movement

The movement of property has been made easier by the rise and growth of the Internet, facilitating wireless transactions, and making the conversion of cash to property and property to cash easier. A director of The Gillette Company testified before the U.S. Congress that 34 million counterfeit Duracell batteries were seized in 2004, along with 31 million fake Gillette shaving products and tens of thousands of fake Oral-B toothbrushes. He estimated a $200 billion loss to the U.S. economy and a loss of 750,000 American jobs, asking Congress to pursue international avenues to promote enactment of mandatory confiscation and destruction laws, strengthened criminal penalties, and enhanced global cooperation on the issue. He further testified that "The majority of goods are stolen not for personal use but by organized criminals intent on the resale of the goods or to use them as collateral for other consumables such as drugs." This is carried out through organized retail theft rings, which "recruit gangs of shoplifters, giving them lists of low-volume, high-value items to be stolen from retail outlets items such as razor blades, batteries, over-the-counter drugs, infant formula, and designer clothing." Those caught are treated as individual shoplifters and are handled leniently, overlooking the organized crime connection behind the crimes (Fox, 2005). This suggests a larger profit motive behind these frauds than personal gain; instead, fraud becomes a self-supporting business with profit potential far beyond that of mere larceny. The scope of harm produced by larceny is usually limited to the value of the physical property taken, whereas fraud often involves re-selling of nonphysical property which has limitless value. For example one Internet posting on a known hacker website read, "I work in the fraud dept. for a well known U.S. company, and have access to hundreds of CCs (credit card numbers) on a daily basis. All I'm looking for is an easy way to make some money and stay anonymous. . . . " He received the first of six inquiries within an hour, describing how to sell and use stolen private information quickly and easily sold over the Internet (Kirby, 2005).

Table 1
Trends in Arrests for Fraud

Year	Number Arrested	Rate per 100,000 Population
1970	76,861	50.7
1980	261,787	125.7
1995	320,046	162.9
2003	208,469	102.2
Totals	+171 %	+ 102 %

Source: FBI, *Crime in the United States.*

Table 1 illustrates that arrests for fraud have increased substantially over the last 30 years. Whether changes in fraud are measured by arrests (up 171 percent) or by the rate of arrests per 100,000 population (+ 102 percent), which accounts for population growth, Table 1 shows a substantial increase over time. But has fraud always been popular?

Protecting Property from Larceny

Perhaps the oldest form of criminal behavior is theft, and it remains the most common crime in all societies of all types. The most common form of theft, historically, has been larceny by stealth—that is, stealing by secretive or furtive means. Property owners over the years have taken great precautions to protect their property. Public police forces did not exist in most countries (including the United States) until the nineteenth century. Prior to that, citizens were responsible for protecting their own property, and they either armed themselves, hired bodyguards, or fashioned "safes" as places to store their valuables. Later in that century, banks became central repositories for valuable private property, when government currency and jewels came to be the primary indicators of wealth and the means for exchange.

The evolution of bank safes offers an interesting example of how theft has changed over time. As is still true today, patterns of theft from banks were strongly related to the available opportunities to steal. During the early twentieth century, safes were locked with a key. Thieves learned how to pick the locks, so the combination lock was invented. Criminals founds a way to pry the entire combination spindle from the safe, so sturdier locks were manufactured.

In an apparent response to this move, safecrackers drilled holes in the safes and inserted explosives to open them. Metals were then alloyed to make safe difficult to violate. Some criminals obtained nitroglycerin, which could be inserted into tiny crevices, or used oxyacetylene torches to open safes. Safes soon appeared with perfectly fitted doors that could not be pried, drilled, melted, or penetrated by explosives.

Some criminals turned to kidnapping bankers, forcing them to open the safes, and the time lock was invented to prevent this. In a similar way, some burglars began to cart away the entire safe to be opened later, and safes were made larger and too heavy to move. Night depositories were also invented to provide businesspersons an alternative to keeping cash in their smaller store safes. Safes were later invented that would release gas when disturbed, so criminals equipped themselves with gas masks (Cressey, 1972).

This progression in the organization of thefts from bank safes illustrates an important factor in the history of theft. There is a relationship between the technology of crime and the technology of prevention. If changes in the nature of safecracking can be generalized to other forms of theft, it may be true that the more sophisticated the prevention technology (e.g., harder metals, time locks, etc.), the more sophisticated criminals must become to maintain acceptable levels of success (e.g., using explosives, kidnapping bankers, etc.).

Credit card fraud has endured a similar progression in frauds and fraud prevention. In the beginning banks that issued credit cards published regular listings of invalid numbers in booklet form, so merchants could see if a submitted card had been stolen or canceled. The response of criminals was to steal a card and use it as any times as possible immediately thereafter to reach the credit limit before the stolen card number was published. Banks responded with magnetic tape readers in stores that communicated electronically with the bank's computer at the point of sale to determine the card's status, eliminating the need for published lists. Some thieves then took an alternate approach and went through store trash bins to retrieve used carbon forms credit-card purchases, which contain an imprint of the owner's account number and signature. This information could then be use to manufacture a duplicate card that would turn up as "valid," when used. More recently, carbonless receipts were developed, and three-dimensional holograms were added to credit cards to make them more difficult to duplicate. The dramatic growth of shopping online via the Internet created the need for the numeric code on the back of credit cards to insure that the online buyer actually had possession of the card being used.

"Dumpster diving used to be the number-one concern," ten years ago, according to director of fraud prevention and data security for American Express. Fraud prevention in that era consisted of tearing up carbon copies of sales slips. "These were very manual ways for people to collect information and perpetrate fraud," she says. "Now it's identity theft, 'phishing,' skimming" (Gardham, 2005). In skimming, thieves use a merchant's credit card reader to capture magnetic-stripe data and then re-encode credit and debit cards. The cards are then given to runners, who shop at malls, high-end jewelry stores, electronics stores, and other retailers. Phishing involves sending individuals an e-mail request for information that appears to come from a legitimate company, store, or bank which asks recipients to verify confidential personal information, such as account numbers, social security numbers, passwords, or other sensitive information. This information is then used to unlawfully

Table 2
The Changing Nature of Theft

Older Manifestations of Theft	Modern Manifestations of Theft
Larceny and burglary (because property usually held on site).	Identity Theft (usually to gain access to the credit line/purchasing power of the owner).
Real property theft (cash, physical property).	Intellectual property theft (patents, trademarks, trade secrets, and copyright).
Pickpocketing and purse snatching (because property and cash often carried by individuals).	Skimming (theft of credit card information by deception, usually via electronic means) or Phishing (false e-mail solicitations to lure a suspect to divulge personal or credit information).
Risk higher (always the possibility of a face-to-face confrontation with the victim and the need to escape quickly from the crime scene to avoid apprehension).	Risk lower (never involves face-to-face contact with the victim, and no need for speed or agility because success requires deception rather than stealth).

use that person's credit or bank account. As was shown above in the case of bank safes, the history of credit card fraud has shown the back-and-forth between the technology of criminals and the technology of law enforcement to keep pace.

Table 2 illustrates the changing nature of theft, depicting how changes in the way we own, store, and move property has changed in the electronic age. Access to cash and merchandise is now done remotely with ease, making possible identity theft, intellectual property theft, skimming and fishing, which have become modern forms of theft (now fraud), because information that provides access to cash or property (e.g., credit card, bank account information) involves less risk and more potential gain than attempts to steal the property directly through burglary or larceny.

Crime Prevention Technology Reacts to Criminal Technology

British sociologist Mary McIntosh has suggested that improvement in crime detection forces criminals to become more organized in order to remain successful. As she explains, "criminals and their opponents are thus engaged in an all-out war which has a tendency to escalate as each side improves its techniques to outwit the other" (McIntosh, 1975: 52). Thieves plan and organize their behavior in order to minimize the risk of a direct confrontation with the victim, which might lead to violence—something almost always found undesirable by offenders. As a result, the primary goal of most thieves is sufficient organization to reduce the possibility of apprehension and, thereby, increase the chances for success.

Rapid changes in the global economy and technology, including worldwide access to the Internet, ease of communications with e-mail and mobile phones, and the rise of electronic buying, selling, and banking without the need for face-to-face transactions, have combined to create new opportunities that can be exploited by motivated offenders. Once thieves experience some success, the government and private industry take steps to reduce the opportunities for theft. This improvement in the detection and/or prevention technology is subsequently matched, and often surpassed, by criminals if they are to avoid apprehension.

Law, law enforcement, and prevention technology usually lag behind the innovative techniques of offenders in exploiting new criminal opportunities. Consider that street lighting is usually improved *after* a number of robberies occur on a dark street. The same can be said for steering-column locks on automobiles, burglar alarms in stores, cameras in banks, and secure safes in all-night convenience stores. It appears that the crime prevention and security technology historically is reactionary to criminal incidents and losses. Only after losses are incurred are improvements made to reduce (or at least change) criminal opportunities. Improved efforts at anticipating changing patterns of theft are needed (see Possamai, 2003; Schuck, 2005).

The dramatic growth in the use and ownership of personal computers during the last 20 years provides another manifestation of new criminal opportunities that were quickly exploited. The invention of the automobile during the early twentieth century has been said to have doubled the number of offenses in the criminal codes of most countries; the invention of the computer likely will have the same effect 100 years later. Automobiles provided opportunities for misuse through untrained operators, manufacturing shortcuts, numerous rules for road usage, complex registration requirements, repair frauds, storage (parking) problems, as well as theft. Computers are having a similar impact as codified offenses are added to eliminate opportunities for misuse such as untrained operators, manufacturing shortcuts, unauthorized usage, registration violations, repair frauds, information storage problems, and theft. Similar to the growth of automobile usage, the growth of computer usage was a threshold event in creating a vast new set of criminal opportunities, which it did not take long to exploit.

The Causes and Prevention of Theft and Fraud

Criminologists try to generalize about why people break the law, although it is has become clear that few adequate generalizations exist to explain criminal conduct such as theft and fraud. Few people steal to survive, and some steal to improve their social standing unlawfully. Some steal to acquire material things they don't actually need, whereas others steal for symbolic reasons involving status, frustration, or revenge. One investigator characterized the causes of fraud in simple terms: "Greed, not misfortune, appears to be the main motivator. Many people think fraudsters are motivated by financial need caused by difficult circumstances —such as illness, divorce or a financial crisis. However, our research shows such causes are

Table 3
Four Approaches to Criminal Behavior

Approach to Crime Causation	Primary Cause of Crime	Prescribed Remedy
Positive	External factors (usually social and economic).	Rehabilitation or reform by changing social and economic conditions, or by changing a person's reaction to them.
Classical	Free-will decision guided by hedonistic tendency to maximize pleasure and minimize pain.	Deterrence through threat of apprehension and punishment.
Structural	Political and economic conditions promote a culture of competitive individualism where personal gain becomes more important than the social good.	More equitable distribution of power and wealth in society, and fewer arbitrary laws, so that all individuals have a greater stake in a better society.
Ethical	Free-will decision guided by ethical principles—illegal conduct occurs because it brings pleasure instead of shame, owing to its wrongfulness and harm to the victim and community.	Education and reinforcement in ethical decision-making from an early age; reduction to the extent possible the external factors that promote unethical decisions.

Source: Albanese, 2004.

only mentioned in a small number of cases" (Gardham, 2005). Contemporary criminologists focus on external factors (positivism), hedonistic pain/pleasure decisions (classical), political and economic factors (structuralism), and ethics (when criminal decisions bring pleasure rather than shame). These schools of thought are summarized in Table 3. A full discussion of these approaches to explaining fraud cannot be conducted here, but it can be seen that different explanations may have relevance depending on the circumstances of the case at hand, and that the causes of fraud have direct implications for its prevention.

Conclusion

Regardless of the source of offender motivation, history suggests that the enforcement technology will always lag behind the criminal technology. Whether bank safes, credit cards, Internet scams, or other kinds of frauds, criminals have exploited opportunities for theft in a manner that exceeds the existing law enforcement technology. Given changes in the ways we hold, store, and move cash and property, fraud has become an easier, more profitable, and less risky way to steal in the twenty-first century. In addition, the opportunities for fraud are increasing, while the odds of apprehension are not keeping pace, resulting in fraud as a growing crime of choice. Whether efforts to prevent fraud in the twenty-first century will effectively limit opportunities, and also provide quick reactions to changes in the criminal technology, remains to be seen. If history is to be a guide, however, the risk of apprehension must be significantly increased beyond current levels, and the available opportunities more effectively circumscribed.

Note

* The points of view expressed are those of the author and do not necessarily reflect the position or policies of the U.S. Department of Justice. Dr. Albanese is chief of the International Center at NIJ on leave from his position as professor of Government and Public Affairs at Virginia Commonwealth University.

References

Albanese, J. (2004). *Organized Crime in Our Times*, 4th ed. Lexis/Nexis/Anderson Publishing.

Associated Press State & Local Wire (2004). "Two Terror Trial Defendants Face New Fraud Charges," 15 December.

Bastian, Lisa D., Patsy Klaus, Craig Perkins, Callie Marie Rennison, and Cheryl Ringel, (2004). *Criminal Victimization*. Washington, D.C. Bureau of Justice Statistics.

Cressey, Donald R., (1972). *Criminal Organization*. New York: Harper & Row.

Federal Bureau of Investigation, (2004). *Crime in the United States*. Washington, D.C.: U.S. Government Printing Office.

Fox, Paul D., (2005). "Organized Crimes Against Manufacturers and Retailers," *Testimony before U.S. House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security*, (March 17, 2005).

Gardham, Duncan, (2005). "Fraud Doubles as Organised Crime Moves In," *The Daily Telegraph (London)*, March 29.

Holmes, Allan, (2005). "Invitation to Steal," *CIO Magazine*, February 1.

Jardini, Nancy J., (2004). "Money Laundering and Terrorism Financing," Criminal Investigation Internal Revenue Service. *Testimony before U.S. House Financial Services Subcommittee on Oversight and Investigations*. June 16.

Kirby, Carrie, (2005). "New, Smarter Generation of Internet Crooks; Personal-information Thieves Hook Up with People Who May Help Them Profit," *San Francisco Chronicle*, April 11, 2005, p. 1.

Krebs, Brian, (2004). "28 Identity Theft Suspects Arrested in Transatlantic Sting," *The Washington Post*, October 29, 2004, p. E5.

Pankratz, Howard, (2004). "10-Year Sentence in 9/11 Scheme," *The Denver Post*, November 5, 2004, p. B4.

Possamai, Mario, (22003). "In It for the Long Haul: Cargo Theft Prevention," *Security Management*, *47* (October 2003), p. 93.

Punch, Linda, (2004). "The New Fraudsters," *Security*, *17*, November, p. 20.

Schuck, Amie M., (2005). "American Crime Prevention: Trends and New Frontiers," *Canadian Journal of Criminology and Criminal Justice*, *47* (April 2005), p. 447.

State News Service, (2004). "Justice Department Announces 'Operation Roaming Charge' Targeting International and Domestic Telemarketing Fraud," 5 October.

U.S. Fed News, (2004). "Ice Task Force Investigation Leads to Indictment of 26," 22 November.

United Nations Interregional Crime and Justice Research Institute, (2004). *Trafficking of Nigerian Girls to Italy*. Turin, Italy: United Nations Interregional Crime and Justice Research Institute.

Warchol, Gregory L., (2004). "The Transnational Illegal Wildlife Trade," *Criminal Justice Studies*, *17*, pp. 57–73.