CHAPTER 1

WHAT IS AN "IDENTITY"?

The term "identity" is commonly used arbitrarily and imprecisely in popular media and literature, and the terms "identity theft" and "identity crime" are frequently used interchangeably. Occasional misuses or misinterpretations are not surprising because in the contemporary context, the traditional meanings underlying those concepts have become increasingly known as information and information technology (IT). Formal definitions of identity concepts are therefore in order.

IDENTITY THEFT VERSUS IDENTITY CRIME

The *Oxford English Dictionary* defines "identity" as "the set of behavioral or personal characteristics by which an individual is recognized." The traditional use of the word "identity" spoke to one's name, familial membership, and occupation (among other applications). The contemporary meaning of "identity" has, however, assumed a candidly IT connotation that extends traditional meanings to include such things as one's consumer and credit histories, financial accounts, and Social Security number. It is this contemporary usage of "identity" that is at issue when it comes to conceptualizing identity theft and identity crime.

Identity theft is a burgeoning crime of relatively recent origin. To be sure, identity theft is dynamic in nature, as it has evolved over time. As

fast as new legislative definitions of identity theft have been framed and novel techniques for enforcing those definitions have emerged, identity predators have abandoned old methods in favor of new and sometimes ingeniously innovative approaches. As the crime has evolved, so also has its descriptions and definitions.

For instance, "identity theft," most commonly thought of as the theft of an individual's *personal* identifying information, has evolved to include a new twist: *business* identity theft.

Further, the theft and fraudulent use of Social Security numbers now assigned babies at birth has, most recently, led to *child* identity theft, much the same way the crime of adult pornography evolved to include those crimes on children. Also similarly, *child* identity theft is now considered a subset of a more general category of crime: *personal* identity theft. Additionally, "identity theft" is defined as a felonious crime per se, that is, as an offense in and of itself, wherein one party steals sensitive information from another, either an individual or a business entity.

Identity *theft*, however, is to be distinguished from identity *crimes*—those offenses committed using the stolen *personal* or *business* identifying information—or "identities." Thus, the conceptual relationship between identity theft and identity crime is that the former facilitates the latter. In short, stolen identities often are used to commit many other crimes, which is why identity theft also can be viewed as an all-encompassing or overarching megacrime. Legislation, investigations, and the prevention of identity theft can take different approaches, depending on the type of identity stolen. Thus, to mitigate and prevent identity thefts requires that each type of identity be clearly delineated: personal, business, and overarching.

"PERSONAL" IDENTITY THEFT

Personal identity theft is the unauthorized acquisition of another individual's personally sensitive identifying information; personal identity *crime* is the use of such information to obtain credit, goods, services, money, or property, or to commit a felony or a misdemeanor. "Personally sensitive

identifying information" means a person's name, address, telephone number, driver's license number, Social Security number, place of employment, employee identification number, demand deposit account number, savings or checking account number, credit card number, or mother's maiden name—information needed to obtain an original birth certification for a complete identity takeover. With a birth certificate, mother's maiden name, and a Social Security number, for example, other governmental documents and records can be accessed; a passport and visas successfully applied for; and driver's licenses, court records, and other information fraudulently obtained and used to commit identity crimes.

Perpetrators use stolen personal identities to drain checking, savings, and retirement accounts; create bogus checks; open new credit card and bank accounts; take over existing accounts; apply for telecommunication and utility services; obtain home, automobile, college-tuition and other loans; open retail accounts; purchase airline, rail, and other transportation accommodations; rent hotel/motel rooms; rent or purchase automobiles; pay for medical supplies, prescriptions, and healthcare services; obtain employment; engage in money laundering, drug trafficking, and other organized crime; and commit acts of terror against the United States. Some, but not all, of these crimes also are committed using stolen business identities, which are to be distinguished from personal identities.

"BUSINESS" IDENTITY THEFT

Business identity theft is the unauthorized acquisition of a business's "business identifying information." Business identity *crime* is the use of such information to obtain credit, goods, services, money, or property, or to commit a felony or misdemeanor. "Business identifying information" means a business's name, address, telephone number, corporate credit card numbers, banking account numbers, federal employer identification number (FEIN), Treasury Identification Number (TIN), State Treasury Number (TN), electronic filing identification number (EFIN: Internal Revenue Service), electronic transmitter identification number

(ETIN: Internal Revenue Service), e-business Web sites, URL addresses, and e-mail addresses.

Business identity theft has become increasingly common for three reasons.

1. Corporate credit card, bank, and other account statements generally have many more entries than the accounts of average individuals and, therefore, are more complex and less easily reconciled.
2. Corporate credit card accounts usually carry higher dollar limits than do individual accounts.
3. Many employees oftentimes are authorized to use a single corporate account. In this case, the theft and fraudulent use of the account number is less easily detected in the corporate credit card statement than in an individual credit statement, which contains fewer account entries.

Alarmingly, the theft of a business's state and federal identifiers has opened the doors to new crimes of business impersonations, such as "subsidiary" fraud. This is the registration, usually with a secretary of state, of a fraudulent subsidiary company using a legitimate business's identifiers. With the payment of a modest registration fee, in some states as little as $25, parasite subsidiary "businesses" can be formed and pose as legitimate businesses, incurring never-to-be-paid expenses for goods and services and obtaining cash through fraudulent business loans and other means. Sometimes these bogus entities defraud legitimate companies by invoicing them for services never rendered or by ordering merchandise that is then sold on the black market.

The most common personal identity crimes are credit card, bank, utilities, telecommunications, and retail (e-business and onsite) fraud. By comparison, the most common forms of business identity crimes are credit card, bank, retail account, and (of most recent origin) subsidiary fraud. These lists are growing. Increasingly, other crimes and new adaptations of crimes are being committed by using stolen identities, both personal and business—which is why the theft of an identity is, in and of itself, an all-encompassing and overarching crime.

IDENTITY THEFT AS AN "OVERARCHING" CRIME

Identity theft is the crime of the twenty-first century, because identity theft is a crime overarching and enabling many other types of crime. For example, stolen identities are used to commit credit card and bank fraud; retail account, utilities, and telecommunications fraud; mortgage and loan fraud; employment fraud; mail fraud; wire fraud; drug trafficking; money laundering; government documents and benefits fraud; prize, sweepstakes, and lottery scams; Internet auction fraud; online stalking and harassment; pornography distribution and consumption; human smuggling (women, children, and illegal immigrants); e-business fraud and a host of other cybercrimes; and terrorism.

According to federal authorities, identity theft is a key catalyst in funding terrorism.[1] Most, if not all, acts of terror against the United States are thought to have been accomplished by the use of fake or stolen identities, including the bombings of the U.S. embassies in Kenya and Tanzania, of the USS *Cole*, of the Marine Corps barracks in Lebanon, of the World Trade Center in 1993, and the atrocities of September 11, 2001. The al Qaeda training manual describes "key missions" that consist of "blasting and destroying" places of amusement, bridges into and out of cities, and embassies.[2] Not mentioned is the conversion of commercial airlines into homicidal guided missiles, although we now know that terrorists also financed these and other attacks using authentic (i.e., stolen versus fabricated) identities, impersonating real people with actual birth and credit records.

In fact, when leaving their training camps in Afghanistan or elsewhere, the "brothers" are provided five discrete sets of identities and given explicit instructions on how and when to use them. For example, when using the identity of a given individual, the impersonator is to speak the language of that individual and dress according to the custom of the individual's identity. Lesson 3 in the al Qaeda manual gives these instructions:

> The brother who has special work status (commander, communication link...) should have more than one identity card and passport. He should learn the contents of each, the nature of the

> (indicated) profession, and the dialect of the residence area listed in the document (p. 22).

In one reported case of identity theft, tens of thousands of foreigners illegally obtained Social Security numbers (SSNs) from the U.S. Social Security Administration.[3] Such an action raises cause for great concern: Once terrorists secure stolen names, addresses, Social Security numbers, and other personal identifiers, they frequently use these identifiers to create bogus passports and driver's licenses, to open bank accounts, to rent automobiles, and to otherwise cover up their nefarious activities. Extremist groups target American businesses and institutions because of the severe financial impact their terrorist acts inflict. Identity theft, therefore, is an overarching crime that enables many other crimes, including terrorism and the devastation it wreaks.

There are no national security standards in place to prevent identity thefts and the resulting wave of identity crimes. Independent businesses are ruined, and, in the aggregate, the financial infrastructure and the very security of our nation are undermined. As will be shown, the effects on people and businesses already have been devastating.