# Topic Page: Identity theft

Definition: **Identity theft** from *The AMA Dictionary of Business and Management*

Crime of stealing another person's identity and financial information for personal gain.

Image from: **Identity theft is often committed for personal...** in *Encyclopedia of Transnational Crime and Justice*

Summary Article: **Identity Theft**
From *Encyclopedia of Business Ethics and Society*

Identity theft, also known as identity fraud, occurs when an individual's personally identifying information is used without permission and/or knowledge by someone else (often a stranger). It is a form of impersonation that enables someone to commit fraud and generally results in financial harm to the individual and financial gain to the impersonator. During the past decade, the increasing amount of personal information available on the Internet has made this a growing concern.

A person's identity refers to that information that distinguishes him or her from other people. In some ways, it encompasses a person's accomplishments and is closely connected to reputation. A person's identity relates to information that exists, whereas a person's reputation reflects opinions about a person's identity.

More specifically, particularly in the context of identity theft, identity refers to the pieces of information that are linked to personal and/or financial value. This set of information comprises both public and private information. For example, a person's telephone number and street address, often available in the public domain, are connected to a person's identity. Confidential information, such as a person's social security number, mother's maiden name, PIN numbers, credit card numbers, and so forth, also contributes to a person's identity. By acquiring access to this information, an individual can impersonate someone else to perform fraudulent transactions, often for financial gain.

Interestingly, there are generally two forms of theft at play. First, there is the theft of the individual's personally identifying information because the information is acquired and/or used without the permission of that individual. The theft that takes place is different from theft of property in that the original owner still has access to his or personal information. The difference is that the value of that information has been depleted because, once misappropriated, it no longer relates uniquely to the original individual but now also points to the imposter as well. Second are the benefits associated with the impersonation. While identity theft is often associated with financial gain (i.e., the theft of money), it can also be used to acquire unauthorized entry, privileges, and/or benefits.

## Techniques

Although identity theft is ostensibly on the rise, it is not a new phenomenon. Prior to the Internet, unscrupulous people stole mail or rummaged through other people's trash (dumpster diving) to obtain personally identifying information such as credit card numbers. Others have been found to have eavesdropped on private conversations in public venues to obtain that sort of information (shoulder surfing). According to a 2003 survey by *Privacy & American Business*, only a small portion of identity theft—16%—is attributable to friends, relatives, or coworkers. People nevertheless remain wary of the

people with whom they do business because anyone to whom you give your credit card or other personal information (i.e., in a bank, store, etc.) has the opportunity to misappropriate that information.

Two new techniques for facilitating identity fraud have emerged as a result of society's growing use of and reliance on the Internet and e-mail. Phishing, for example, occurs when someone impersonates a trusted entity in electronic messages aimed at securing confidential information such as log-in names and passwords. For example, some phishing attempts target the customers of banks and online payment services such as PayPal. These messages often urge individuals to log on to their accounts via provided Web links. In fact, the Web links are fake, and the messages end up tricking people into disclosing their personal information to strangers. The Web links are actually tools used by phishers to capture the desired personal information (i.e., account numbers, passwords, etc.) so that they can then use that information for their own purposes.

The second way in which e-mail and the Internet are exploited for fraudulent purposes is through spam. Spam refers to unwanted, unsolicited e-mail messages, often used for mass advertising. Fraud can occur through spam e-mail as mass messages are used to cheat people by enticing them to buy fake products or pay a fee for a useless or nonexistent service or luring them in some other way to give up money under false pretenses. Many of these messages direct recipients to Web sites that invite them to input personal information in exchange for the opportunity to receive gifts or win awards. These range from a $50 gift card of a department store to a chance in a lottery.

Technology has added new dimensions to concerns surrounding identity fraud. The increasing amount of personally identifying information that is created, exchanged, stored, and maintained in computer-based databases creates new vulnerabilities. The Internet provides a virtual playground for hackers, as do personal computers—used in most offices today. The skillful thief can rifle through electronic data to find what he or she needs without authorization.

## Impact

Within recent years, it appears that, while the number of reported instances of identity theft has arguably decreased, the magnitude of financial harm has increased. According to a 2006 survey cosponsored by Javelin Strategy and Research and the Better Business Bureau, the actual number of adult victims of identity fraud in the United States has decreased from 10.1 million in 2003 to 8.9 million in 2006. The dollar amount suffered by victims as an aggregate has, however, increased from $53.2 billion in 2003 to $56.6 billion in 2006. This is in addition to significant outof-pocket expenses reported by victims that increase losses by 10% or more.

Tremendous tangible and intangible costs are borne by both victims and businesses. The costs to individual victims, in addition to the dollar amount of actual losses, remain significant. Along with financial consequences, victims also suffer damage to their reputation and credit report and substantial lost time. According to a recent survey issued by the Federal Trade Commission (FTC), 15% of victims reported that their personally identifying information was misappropriated for use in nonfinancial ways, such as to obtain government documents.

According to a 2003 survey conducted by the Identity Theft Resource Center, victims on average spend 600 hours regaining their identities and repairing the harm. This same survey reports that the emotional harm associated with identity theft is equivalent to that experienced by victims of violent crimes.

Major costs accrue to financial institutions and other businesses as well. Business losses attributable to identity theft totaled $47.6 billion in 2002, according to the FTC survey. These financial costs are in addition to costs associated with loss of trust and damage to reputation. Additional costs are linked to increased security measures that businesses are finding it necessary to implement to protect the personal information of customers as much as possible.

Account hijacking (i.e., unauthorized access of bank accounts) is reportedly the fastest growing form of identity theft, according to the 2003 Identity Theft Resource Center survey.

## Legal Framework

Identity theft is a crime. That having been said, from a legal perspective it remains a sort of moving target in that it transcends physical, geographic boundaries. It is also difficult to prove. While an individual can claim losses, those losses are not always attributable to a clearly identifiable person, particularly since the thief operates under the guise of a stolen identity. In the United States, local, state, and federal enforcement agencies handle investigation and prosecution under general laws.

Specific privacy and data protection legislation exists in other countries to offer protection from and compensation for identity theft. In Australia, for example, control over identity theft falls under the auspices of the Office of the Privacy Commissioner. In the United Kingdom, personal data are protected by the Data Protection Act, a British act of Parliament that governs proper use of personal data collected and used by organizations.

## Responsibilities of Individuals and Businesses

There is no doubt that the victims of identity theft suffer significant unsolicited harm. It is also true, however, that some victims leave themselves vulnerable to this sort of harm. People who value their personal information have an obligation to take reasonable precautions to protect that information, if for no other reason than that, in many instances, they are in the best position to keep that information secure. All sorts of shredders and shredding services are available today to prevent dumpster divers from acquiring anything useful relating to a person's identity. Furthermore, Internet users can choose what information to reveal online and under what circumstances. Any individual who discloses personal information on nonsecure Web sites does so at his or her own risk.

This is not to say that individuals are always in a position to prevent the theft of their personally identifying information. In fact, according to the FTC survey, 49% of the victims of identity theft do not know how their information was stolen. People can, however, remain vigilant regarding the security of their identities. Regular monitoring of accounts, for example, can provide for early detection of suspicious behavior. Approximately 26% of the victims only become aware of the theft because of reports of suspicious activity by businesses (i.e., credit card companies, banks, etc.).

The arguably greater responsibility therefore falls on the shoulders of businesses. First, it is the responsibility of companies that gain access to personally identifying information to protect that information from unauthorized disclosure. This means that companies have to take particular care in choosing the people they hire and in training them to safeguard customer privacy. In addition, they have an obligation to create and implement systems to protect data from theft.

Second, it is also the responsibility of companies to monitor accounts to detect suspicious activity. American Express regularly verifies unusually large purchases with the account holder before authorizing payment. Similarly, Discover often requires account holder verification after several subsequent gas

purchases in a short period of time. Self-serve payment systems, such as gas stations, are particularly vulnerable to accepting stolen credit cards. While this creates an inconvenience for automobile travelers, it represents one way Discover is able to mitigate losses linked to stolen credit cards.

## Conclusion

The harm to individuals and businesses resulting from identity theft is significant and sometimes irreparable. Once a person's identity is stolen, while he or she can recover financial compensation, the associated emotional damages are much more difficult to repair. Businesses, too, suffer substantial costs linked to identity theft. Although a legal framework aims to prevent and punish identity theft, it nevertheless remains the responsibility of individuals and businesses to safeguard the personally identifying information in their care.

*See also*

Electronic Commerce; European Union Directive on Privacy and Electronic Communications; Internet and Computing Legislation; Privacy; Reputation Management

### Further Readings


- Anderson, K. B. Who are the victims of identity theft? The effect of demographics. Journal of Public Policy & Marketing, 25(2), (2006). 160-171.
- Bauknight, T. Z. The newest Internet scams. Business & Economic Review, 52(1), (2005). 19-21.
- Krause, J. Stolen lives. ABA Journal, 92(3), (2006). 36-64.
- Smith, D. A. The still growing problem of data breach and identity theft. Banking Law Journal, 123(10), (2006). 919-924.
- White, A. E. The recognition of a negligence cause of action for victims of identity theft: Someone stole my identity, now who is going to pay for it? Marquette Law Review, 88(4), (2005). 847-866.


Tara J. Radin



SAGE *Copyright © 2008 by SAGE Publications, Inc.*

## APA

Radin, T. J. (2008). Identity theft. In R. W. Kolb, *Encyclopedia of business ethics and society*. Thousand Oaks, CA: Sage Publications. Retrieved from https://search.credoreference.com/content/topic/identity_theft

## Chicago

Radin, Tara J. "Identity Theft." In *Encyclopedia of Business Ethics and Society*, by Robert W. Kolb. Sage Publications, 2008. https://search.credoreference.com/content/topic/identity_theft

## Harvard

Radin, T.J. (2008). Identity theft. In R.W. Kolb, *Encyclopedia of business ethics and society*. [Online]. Thousand Oaks: Sage Publications. Available from: https://search.credoreference.com/content/topic/identity_theft [Accessed 18 September 2019].

## MLA

Radin, Tara J. "Identity Theft." *Encyclopedia of Business Ethics and Society*, Robert W. Kolb, Sage Publications, 1st edition, 2008. *Credo Reference*, https://search.credoreference.com/content/topic/identity_theft. Accessed 18 Sep. 2019.