

*2009 ASCUE Proceedings*  
**Identification, Causes, and Prevention of Identity Theft**

**Thomas A. Pollack**  
**Duquesne University**  
**600 Forbes Avenue**  
**Pittsburgh, PA 15282**  
**412.396.1639**  
**pollack@duq.edu**

**Abstract:**

The ease of accessibility to personal information has become an increasingly worrisome concern in today's organizations and homes. Crimes of identity theft in which thieves use the victim's personal information to impersonate the victim have become all too prevalent. It is estimated that the number of identity theft victims annually is in the millions. Since identity theft can be a life-changing crime, this is a very serious matter. Although identity theft cannot be eliminated, it can be controlled, to an extent, by taking preventive measures. A great deal of the responsibility for prevention falls on the organization's information systems professionals. From an organizational perspective, precautions must be taken in dealing with the countless records that contain personal information. Of course, individuals must also take precautions to safeguard their confidential information. It is therefore important for information systems managers, general business managers, and individuals to understand information privacy and security along with relevant laws and government regulations. Since many of the theft controls and measures to combat identity theft are achieved through systems and technology, students in technology-related fields also need to be aware of both the technical and legal safeguards that are intended to protect the privacy and security of information. General and technical managers must stay apprised of current trends and practices regarding identity theft and know what to do in the event of an identity theft occurrence. This paper will discuss many of the technical, legal, and regulatory measures that are intended to help avoid identity theft.

**Introduction**

Identity theft has become a major problem in the United States and around the world; a problem that cannot be eliminated but one which can be better controlled by taking appropriate measures.

Simply defined, identity theft is a crime in which the thief uses the victim's personal identifying information such as a driver's license number or social security number to impersonate the victim (Pearlson, p.258). It is the unlawful use of another's identifying information for gain, and it has become the most prevalent financial crime in the United States (White, 2008).

Identity theft can be a life-altering experience. The U.S. Federal Trade Commission (FTC) estimates that consumers lose up to \$50 billion annually to identity theft and recovery expenses. Victims are generally not held responsible for the fraudulent charges that result from identity theft, but the costs for the victim far exceed the monetary losses of the crime. Many experience a range of emotional states that mirror post-traumatic stress disorder, including denial, anger, guilt, shame and embarrassment, fear and a feeling of being violated (White, 2008). The Javelin

## ***2009 ASCUE Proceedings***

Strategy and Research Center has been studying identity theft since 2004, and their findings estimate that identity theft crimes affected almost 10 million victims in 2008, an increase of 22% over 2007 (Spendonlife.com, 2009). The FTC reported that its consumer fraud and identity theft complaints in 2007 showed a 21% increase over 2006. Unfortunately, many people do not realize that they have been victimized for months or even years. However, it is estimated that 71% of fraud occurs within a week of a victim's personal data being stolen (Spendonlife.com, 2009). In the meantime, thieves are accumulating debts, committing crimes, ruining credit records, etc. The FTC also estimated that U.S. businesses and financial institutions are losing about \$53 billion annually as a result of identity theft (Swartz, 2009). The average cost for an organization per record compromised is about \$197, typically for phone calls, free credit monitoring and discounts on membership fees and merchandise (Prosch, 2009).

### **Legislative Measures**

The United States recognized identity theft as a crime in 1998 when the Identity Theft and Assumption Deterrence Act (ITADA) was passed. ITADA issued a general definition for identity theft as the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime.

The ITADA definition takes into account three types of identity theft. In general terms, they include:

1. New account theft – Occurs when multiple pieces of information about someone is stolen, and the thief assumes the victim's identity;
2. Existing account theft – Occurs when something is stolen from some existing financial account;
3. Synthetic identity theft – Occurs when stolen information is combined with financial information to create a new fake identity (Schreft, 2007).

White (2008) also classifies three types of identity theft using definitions slightly different from the above, but nevertheless quite familiar. They include:

1. Financial identity theft – Occurs when the identity thief uses a victim's personal information to withdraw money or open a bank account or use a credit card or other type of credit in the victim's name;
2. Nonfinancial identity theft – Occurs when the thief uses the victim's information to obtain health benefits, commit fraud or receive a service;
3. Criminal record identity theft – Occurs when the thief commits crimes, traffic violations, or other illegal activities acting as the victim.

From the above classifications, one can readily see that there are a number of ways to classify identity theft and also understand the seriousness and the life-altering potential of becoming an identity theft victim. Statistics indicate that identity theft continues to be on the rise, and it is certainly a crime that must be taken seriously. Since it is the most prevalent financial crime in the U.S., it warrants the attention and precautionary actions of consumers, as well as business and government officials.

## *2009 ASCUE Proceedings*

Another piece of legislation that addressed the need to protect information privacy was passed in 1999. The Gramm-Leach-Bliley Act of 1999 (also referred to as the Financial Services Modernization Act) requires financial institutions to ensure the security and confidentiality of personal information (names, addresses, social security numbers, credit card numbers, credit histories, etc.) and contains a fraudulent access to financial information section (FAFI), which directs financial institutions, such as banks and investment companies, to have “policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and deter fraudulent access to such information” (White, 2008).

Also somewhat related, is the Computer Fraud and Abuse Act of 2001. The act “describes various computer crime offenses that include intentionally accessing a computer without authorization or exceeding authorized access to obtain financial and credit card information” (White).

Several years later, in 2003, the Fair and Accurate Credit Transactions Act was passed and includes provisions such as the following to prevent identity theft (Haag, 2008).

- Consumer’s have a right to get a free credit report once per year;
- Merchants are required to leave all but the last five digits of a credit card number off the receipt;
- Lenders and credit agencies are required to take action if there is a suspicion of identity theft.

Although identity theft was becoming prevalent in 2003, consumers rarely heard of these thefts. That changed after a landmark California law called the Security Breach Notice Law was passed in 2002. The law, which set off a series of nationwide events, went into effect in mid-2003, and it requires businesses or state agencies that experience a security breach to notify state residents if their personal information is lost or stolen (Greenberg, 2008). After ChoicePoint, a company that collects and compiles information about millions of consumers, inadvertently sold the personal information of 145,000 people to a Los Angeles con artist, lawmakers in other states moved quickly to ensure that their citizens would receive the same kind of notice as California residents. Nearly all states now have similar laws (Greenberg). Thus, once notices began to be sent on a widespread basis, identity theft became a part of the American culture and became a dreaded term in our vocabulary.

Many identity theft and fraud cases are prosecuted by the Department of Justice (DOJ), largely under the earlier mentioned Identity Theft and Assumption Deterrence Act (ITADA). Examples of federal offense felonies that carry substantial penalties include identification fraud, credit card fraud, and financial institution fraud. Some of the above offenses carry penalties as high as 30 years’ imprisonment, fines, and criminal forfeiture. Federal prosecutors work with federal investigative agencies such as the Federal Bureau of Investigation, U.S. Secret Service and the U.S. Postal Service to prosecute identity theft and fraud cases (U.S. Department of Justice, 2009).

The information in the preceding paragraphs describes legislation that has been passed at the federal level. However, a great number of identity theft prosecutions occur at the state level, and state law then serves as the foundation. At least 48 states have identity theft laws, but there is significant variation in several important areas. State to State areas of variation on identity theft include the following:

## *2009 ASCUE Proceedings*

- **Felony vs. misdemeanor** – Some consider identity theft a felony, some a misdemeanor, and some base it on the amount stolen.
- **Repeat offender** – Some prescribe harsher punishment for repeat offenders.
- **Victim assistance** – Some have provisions to ensure judicial relief to clear victims' names.
- **Venue** – Some prosecute regardless of jurisdiction, others only if the crime is within their jurisdiction.
- **Statute of limitations** – Most do not address when the statute of limitations begins.
- **Reverse criminal record identity theft** – Most fail to address this (using victim's good name to secure employment because of an existing criminal record) (White, 2008).

States' failure to model their identity theft legislation after ITADA has produced a great deal of inconsistency in state level occurrences, punishments and strategies to target identity theft occurrences (White).

## **Identity Theft Tactics**

Identity theft can occur in a variety of ways, and for the most part, the general public is unsuspecting. We have come to think of identity theft as theft that involves sophisticated technology and highly trained criminals, but a great deal of identity theft occurs as a result of low-tech crimes such as check forgery, credit card misuse, employee negligence and the use of information carelessly thrown into the trash. A comprehensive list of the most common identity theft tactics has been compiled by Credit.com (2009):

The list includes the following:

- **Check fraud** – Printing fake checks, stealing checks, ordering checks in someone's name or tampering with real checks.
- **Dumpster diving** – Stealing documents from a person's or business' trash can. Sensitive documents should be shredded.
- **Account redirection** – By filing a simple change of address form with the post office or by contacting your creditors, an identity thief can have an individual's personal mail sent to his or her own address.
- **Internal theft** – Employees of loan offices, credit agencies and companies that deal with sensitive data can steal records and use them for identity theft.
- **Purse/wallet snatching** – Theft of a wallet or purse.
- **Mail theft** – Steal mail from a person's mailbox in order to get credit card applications and other sensitive data.
- **Data theft** – Theft of consumer files from businesses, doctor's offices, universities, lenders, etc.
- **Child fraud** – Stealing the identity of a child and using his or her positive credit history to open accounts.

### *2009 ASCUE Proceedings*

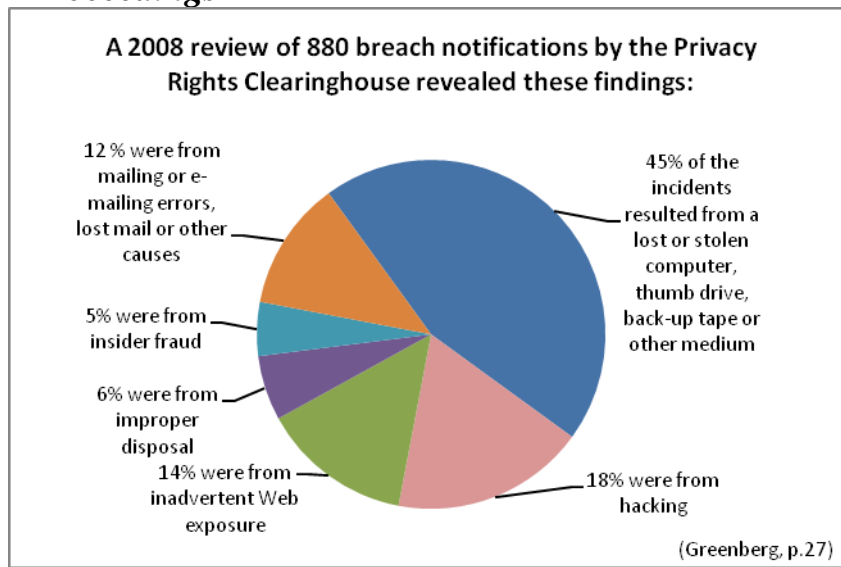
- **Computer spyware** – Spyware can be installed on an individual's computer without the individual knowing it. Every keystroke and word typed and website visited can be recorded and transmitted.
- **Social Security fraud** – Use of fake Social Security Numbers, including the numbers of people who have recently died.
- **Pretexting** – Thief contacts a financial institution posing as a customer and requests the customer's account information.
- **Insider Theft** – Employees or subcontractors can be the source. Up to 88% of insider theft may be inadvertent and the result of employee carelessness and negligence (Brandel, 2009).

Some of the more recent technology-related tactics used by identity thieves to steal consumer data and which are growing in popularity, include the following:

- **Phishing** – Emails are designed to look like an official message from a bank or financial website and requests an individual to update account information such as name, address, account number, PIN, and social security number. Can also occur over the phone.
- **Pharming** – Variation on phishing whereby thieves set up fake websites that look like official organization websites in order to “pharm” consumer data. Victim is directed to a fake site that looks real and asked to enter personal information.
- **Skimming** – Thieves use tiny hand-held credit card readers to collect information recorded on the magnetic strips of credit cards. Common in restaurants and stores where individuals submit a credit card to make payment.
- **Wireless hacking** – Thieves access personal data by tapping into these wireless connections. When a wireless network or Bluetooth system isn't secure and encrypted, individuals are susceptible (Credit.com, 2009).

As one can readily see from the chart that follows, statistics compiled by the Privacy Rights Clearinghouse reveal that although tactics varied widely, nearly 80% of the personal information breach notifications received in 2008 were technology-related. The Privacy Rights Clearinghouse further revealed that about 75% of the publicly known breaches reported involved social security numbers (Greenberg, 2008). Thus, it is extremely important for today's systems managers to have knowledge of common identity theft tactics and exercise extreme caution in systems design, operation and monitoring.

## 2009 ASCUE Proceedings



### Governmental Preventive Measures

Throughout much of the world, governments have generally relied on two key means of identity protection. Cards or documents such as passports and driver's licenses and unique identifiers such as passwords or personally unique numbers such as social security numbers have been used for verification and authentication. Neither means is particularly effective. Cards and documents can be forged or counterfeited, and numbers are frequently lost or forgotten. Passwords as identifiers have become pervasive, and the cost of maintaining and controlling them has become exorbitant. Add to this the fact that not all authenticators who control these passwords are honest individuals, and unfortunately they have access to a host of confidential identity information (Chertoff, 2009).

Measures are being taken to make it much more difficult to counterfeit or forge cards or documents. Techniques such as chips in passports, the creation of secure pass cards, the use of bar codes, and embedded holograms in identification documents are enhancing the security of cards and documents. In the U.S., as a result of the REAL ID initiative, uniform standards are being established for all states to follow as they create driver's licenses and other state-related documents. Improved encryption techniques are also being used to safeguard numerical authenticators such as social security or PIN numbers (Chertoff, 2009).

The Federal Trade Commission (FTC) released recommendations to congress to help prevent identity theft through use of social security numbers on December 17, 2008. These recommendations followed a period of extensive research and included the following five points:

1. Develop a national standard to improve consumer authentication;
2. Restrict public display (posting) and transmission of social security numbers;

### *2009 ASCUE Proceedings*

3. Establish national standards for data protection and customer notification regarding security breaches;
4. Increase education and outreach efforts to businesses and consumers on what can be done to reduce use and increase protection of social security numbers; and
5. Improve coordination and information sharing between private sector entities and government agencies to establish best practices (Adams, 2009).

The FTC also hopes to reduce losses attributed to identity theft with an update to the Fair and Accurate Transactions Act (FACTA) of 2003 with a program called the “Identity Theft Red Flag” program. Program enforcement will begin May 1, 2009. Fundamentally, to meet the new requirements, all organizations that handle consumer credit accounts must conduct an identity theft assessment and develop measures to identify, mitigate and prevent theft of consumer data (Swartz, 2009). Specifically, the requirements issued by the FTC apply to Section 114 of the FACTA Identity Theft Red Flags. There are 27 red flags that fall into the following five categories:

1. Alerts, notifications, or warnings from a consumer reporting agency;
2. Suspicious documents;
3. Suspicious personally identifying information;
4. Unusual use or activity relating to a covered account;
5. Notices from customers, identity theft victims, law enforcements officials, or other businesses about possible identity theft relating to covered accounts (Swartz 2009).

Stated simply, the red flag rules will force financial institutions to authenticate customers’ identities and be more diligent in analyzing consumer transactions with the goal of being better able to protect sensitive customer information (Swartz).

### **Business Preventive Measures**

Thus far this paper has presented some of the federal legislation that has been enacted to assist in our efforts to deter identity theft. Businesses also play a critical role in recognizing and deterring identity thieves. The American Institute of Certified Public Accountants (AICPA) has produced a comprehensive list of 10 suggestions for businesses to follow to avoid identity theft. The list of suggestions to safeguard personal information (PI) is as follows:

1. Do not collect more PI than you need
  - Document the types of PI you collect
  - Analyze PI being collected to determine if it is necessary to deliver your services
  - Document systems, business processes, and transactions that collect PI

## ***2009 ASCUE Proceedings***

2. Do not retain PI longer than legally required and/or necessary for business purposes
  - Determine legal requirements for record retention
  - Identify business purposes for retaining PI, and establish retention requirements
  - Document where PI is retained
  - Establish rules for purging PI
3. Protect PI you collect, use, disclose and retain
  - Establish administrative safeguards
  - Establish technical safeguards for logical access controls
  - Establish technical safeguards for identity management
  - Establish technical safeguards for network security
  - Establish technical safeguards and document policies for updating security patches and anti-virus software
  - Maintain security of physical mediums
4. Ensure additional protection methods on sensitive PI retained
  - Determine the type of sensitive PI to secure
  - Determine the required level of security
  - Identify where encryption solutions may be needed
5. Restrict access to PI only to individuals who have a business need to access information
  - Restrict Access to PI
  - Challenge the need to access PI for positions in an organization
6. Dispose of PI appropriately
  - Develop policies and procedures for disposal
7. Instill awareness and train employees on the proper handling of PI
  - Develop a privacy awareness program
  - Identify responsibility for providing training
  - Document training records
8. Understand federal, state and local laws
  - Know federal state and local laws and the rights consumers and employees have under those laws
9. Conduct regular audits to ensure PI is protected
  - Identify responsibility for monitoring the protection of PI
10. Keep abreast of the latest information on protecting PI
  - Generally Accepted Privacy Principles (GAPP)
  - Comparison of international privacy concepts (AICPA, 2008)

## *2009 ASCUE Proceedings*

Businesses also need to be aware of the Data Life Cycle Management (DLCM) process; that is the flow of data from its creation to the point when it has lost its business value to the organization (but not necessarily its value to data thieves). Attentiveness to this cycle can help avoid thefts and unwanted exposure of information. The DLCM consists of the following five phases:

1. Data Collection and Transmission – Focus on the security and necessity of collecting PI;
2. Data Storage – Focus on unauthorized access by both internal and external sources;
3. Data Processing and Use – Focus on safeguards against information being erroneously processed and accidentally exposed;
4. Data Sharing and Replication – Focus on development and enforcement of policies and have appropriate training in place and
5. Data Destruction – Focus on appropriate destruction of paper-based and electronic PI (Prosch, 2009).

If an organization experiences a PI breach, it must be prepared to take action immediately. That means an Incident Response Plan and Team must be in place. This team is responsible for putting the plan into action very quickly and therefore must be well-trained. When a PI breach has been confirmed, the affected individuals must be notified as quickly as possible. The steps should be as follows:

1. Notify the Incident Response Team;
2. Coordinate timing, content, and notification method with chief privacy officer and legal counsel;
3. If desired, prepare and issue a press release (press will find out);
4. Be proactive in notifying the affected individuals and the public (Prosch, 2009).

Failure to act swiftly and properly can result in sanctions by the FTC. If a company is sanctioned, it will incur the added cost of required security audits every two years for the next 10 to 20 years (Greenberg, 2008).

In addition to commonly used defenses such as spyware detection software, encryption methodologies and effective firewalls, businesses need to take special precautions to protect the personal information stored in their vast array of databases. As referenced above, many organizations have hired a Chief Privacy Office to provide oversight in the increasingly important area. Organizations are also enhancing training and awareness programs in an effort to prevent internal theft and employee negligence incidents.

### **Individual Preventive Measures**

As stated previously, if one becomes a victim of identity theft, the experience can prove to be life-altering. Correcting damage done by criminals against an individual's name, reputation, personal or financial status, etc. can be a very daunting task. Some basic steps for minimizing identity theft or fraud can be summarized by remembering the word “**SCAM**” (U.S. Department of Justice, 2009).

- S** Be **stingy** about giving out your personal information to others unless you have a reason to trust them, regardless of where you are:
- Adopt a “need to know” approach to your personal data.

## ***2009 ASCUE Proceedings***

- If someone you don't know calls you on the telephone and offers something of value, but asks you for personal data, ask them to send you a written application form.
  - If they won't do it, tell them you're not interested and hang up.
  - If they will, review the application carefully when you receive it. The Better Business Bureau can give you information about businesses that have been the subject of complaints.
- If you're traveling, have your mail held at the post office.
- If you have to telephone someone while you're traveling and need to convey personal financial information, do it privately.

### **C Check** your financial information regularly, and look for what should be there and what should not be there.

- What should be there – monthly bank and credit card statements.
  - If you're not receiving monthly statements, call the financial institution immediately.
  - If your statements are being mailed to another address that you haven't authorized, tell the financial institution or credit card representative immediately that you did not authorize the change of address.
- What shouldn't be there – checking your monthly statements carefully maybe the quickest way to find out if someone has gotten your financial data.
  - If someone has managed to get access to your mail and other personal data, and opened any credit cards in your name or taken any funds from your bank account, contact your financial institution or credit card company immediately.

### **A Ask** periodically for a copy of your credit report.

- Your credit report should list all bank and financial accounts under your name, and it will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

### **M Maintain** careful records of your banking and financial accounts

- Retain your monthly statement and checks for at least one year.

If you actually have the unfortunate experience of becoming a victim of identity theft, the U.S. Department of Justice (2009) suggests the following actions:

- Contact the Federal Trade Commission (FTC) by telephone toll-free at 1-877-ID THEFT (877-438-4338) to report the situation

Under the Identity Theft and Assumption Deterrence Act (ITADA), the Federal Trade Commission (FTC) is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement.

## *2009 ASCUE Proceedings*

You may also need to contact other agencies for other types of identity theft:

- Your local office of the Postal Inspection Service
- The Social Security Administration
- Internal Revenue Service (call 1-800-829-0433)

Also, call the fraud units of the three principal credit reporting companies:

1. Equifax – call (800)525-6285
2. Experian – call (888) EXPERIAN or (888)397-3742
3. Trans Union – call (800)680-7289

Contact all creditors with whom your name or identifying data have been fraudulently used.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge.

Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief. If you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

1. CheckRite – 800-766-2748
2. ChexSystems – 800-428-9623 (closed checking accounts)
3. CrossCheck – 800-552-1900
4. Equifax – 800-437-5120
5. National Processing Co. (NPC) – 800-526-5380
6. SCAN – 800-262-7771
7. TeleCheck – 800-710-9898

### **Conclusion**

Identity theft is a crime that is growing rapidly and one which costs the U.S. economy billions of dollars per year. Unfortunately, data breaches have become a way of life for corporate America (Brandel, 2009). Thieves are continually developing more sophisticated schemes, and forcing our government, businesses and individuals to enhance their awareness and protection practices against this devastating crime.

Old fashioned thievery tactics have given way to more sophisticated, technology-based schemes for theft of personal data. The end result is that personal information is stolen in large volumes and thousands of people can be affected. The magnitude of crimes involving identity theft is such that our government, through legislation, our businesses, through improved processes, and individuals, through enhanced knowledge and understanding, must all do their part to curtail the increasing number of incidents. From a governmental perspective, the Department of Justice, and from an organizational perspective, the American Institute of Certified Public Accountants have produced valuable guidelines to both prevent

## ***2009 ASCUE Proceedings***

and deal with identity theft. As a result of legislation, when personal information breaches do occur, organizations are faced with the daunting task of notifying potential victims as soon as possible. Of course, for an organization to be prepared to deal with a breach of personal information, planning is important. If organizations adopt a mix of computer technology, internal controls, contractual agreements, and assigned responsibilities, they can help prevent identity theft, take prompt corrective action and minimize their liability (Petravick, 2009).

From a need to know perspective, it is important for individuals to understand how identity theft occurs and possess knowledge of what one should do if victimized by this extremely intrusive crime. As educators prepare students to assume positions in organizational environments, they must incorporate “real world” issues into their educational offerings. It is not enough for prospective computer and systems professionals to be proficient in technical issues such as programming and analysis. They must possess a sense of awareness of issues that they will face on a day-to-day basis as professionals. Frequently, these issues are not evident in the textbook being used for a course. It is therefore imperative that the coverage of matters such as identity theft (and how to deal with it) be introduced as part of the knowledge base of the instructor. Typically, this means extending instruction beyond the boundaries established by a typical programming or systems textbook. It is important, therefore, for the instructor to be knowledgeable of these issues and their associated implications and legalities.

## **References**

- Adams, K. (2009). Information security. *Collector*, 74(7), 32. Accessed 3/16/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1636209231&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- AICPA. (2008). *Identity theft presentation with speaker notes*. Accessed 3/26/2009 from <http://infotech.aicpa.org/Resources/Privacy/Privacy+Hot+Topics/Identity+Theft/>
- Brandel, M. (2009). Blindsided! *Computerworld*, 43(6), 27-31
- Chertoff, M. (2009). Managing identity: A global challenge. *Orbis*, 53(1), 137. Accessed 3/17/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1630681471&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- Credit.com. (2009). *Identity theft basics*. Accessed 3/18/2009 from <http://www.credit.com/products/security/Identity-Theft-Basics.jsp>
- Greenberg, P. (2008). Right to know. *State Legislatures*, 34(10), 26. Accessed 3/16/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1609896871&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- Haag, S., Baltzan, P., & Phillips, A. (2008). *Business driven technology* (2<sup>nd</sup> ed.) Boston, MA: McGraw-Hill Irwin.

### **2009 ASCUE Proceedings**

- Pearlson, Keri E., & Saunders, Carol. (2000). *Managing and using information systems: A strategic approach* (4<sup>th</sup> ed.) Hoboken, NJ: John Wiley & Sons, Inc.
- Petravick, S., & Petravick, G. (2008). Understanding litigation risks associated with identity theft. *The CPA Journal*, 78(10), 66. Accessed 3/17/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1585902141&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- Prosch, M. (2009). Preventing identity theft throughout the data life cycle. *Journal of Accountancy*, 207(1), 58. Accessed 1/30/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1626526461&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- Schreft, S. L. (2007). Risks of identity theft: Can the market protect the payment system? *Economic Review - Federal Reserve Bank of Kansas City*, 92(4), 5. Accessed 3/17/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1447833331&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- Spendonlife.com (2009). *2009 Identity theft statistics*. Accessed 3/17/2009 from <http://www.spendonlife.com/guide/2009-identity-theft-statistics>
- Swartz, N. (2009). Will red flags detour ID theft? *Information Management Journal*, 43(1), 38. Accessed 1/30/2009 from <http://proquest.umi.com/authenticate.library.duq.edu/pqdweb?did=1635159201&Fmt=7&clientId=3262&RQT=309&VName=PQD>
- U.S. Department of Justice. (2009). *Identity theft and identity fraud*. Accessed 3/18/2009 from <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>
- White, M. D., & Fisher, C. (2008). Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review*, 19(1), 3.