UW E-Business Consortium
University of Wisconsin-Madison

# Combating Identity Theft:

***Leading Practices for Credit Unions***

**Stephen Lloyd Arnold**
Researcher and Consultant
SLArnold@Wisc.edu

**Alfonso Gutierrez**
Associate Director, Research and Education
AGutierr@Wisc.edu

**Jason Hurd**
Project Assistant

October 2007

# 1. Introduction

## 1.1 Motivation and Objectives of this Study

Identity theft has a significant negative impact on individual consumers, companies, and the country itself. In the United States in 2006, $56.6 billion dollars were stolen through identity theft. Average fraud per victim in the U.S. was $6,278 in 2006 (Privacy Clearing House, 2007). Much of the loss is covered by businesses. In 2004, businesses reported average monetary losses of $49,254 (Identity Theft Resource Center, 2007).

For victims of identity theft – both individual consumers and companies – the costs extend beyond financial losses. Indirect and nonfinancial costs include time and reputation, damage to credit records, corruption of personal information in corporate and government databases, and wrongful arrest. The effects of identity theft are so disturbing to both individuals and affected organizations that there is significant underreporting of the crime. It is, therefore, important to build awareness and promote adoption of practices that can proactively help prevent identity theft.

This study, conducted by the UW E-Business Consortium, in cooperation with CUNA Mutual, CUNA, and the Credit Union Information Security Professionals Association, is intended to help credit union executives make informed decisions on how to focus efforts to minimize the chances of identity theft.

The primary objectives of this study were to:

1. Clearly define identity theft and the types of identity theft,
2. Characterize how **sensitive personal information (SPI)** is usually compromised,
3. Determine how much SPI lost via each route is actually being used to commit fraud,
4. Describe threats and defenses using attack tree diagrams, and
5. Use these results to recommend where identity theft prevention efforts should be focused.

The insights shared in this report are based on our analysis and interpretation of various published data and reports on identity theft incidents as well as information gathered (via interviews and focus group discussions) from information security professionals and executives in the credit union industry.

## 1.2 Identity Theft: Definition and Types

Identity theft has become an increasing problem and concern for companies and consumers across the country. In fact, there are approximately 10 million people who are victims of identity theft per year (Identity Theft Resource Center, 2006). Identity theft occurs when someone wrongfully acquires or uses another person's SPI (such as name, social security number, address, and bank account numbers) and this breach of privacy allows for possible gain through fraud. Some refer to identity theft as identity fraud, since the "thief" does not deprive the victim of his or her identity (Wikipedia, 2007).

There are many different types of identity theft. The most common types of identity theft include check fraud, credit card fraud, mortgage fraud, and other kinds of financial and bank fraud. Each of these types of identity theft involves fraudulent financial gain. Less commonly, identity theft includes employment fraud (obtaining a job by using a victim's name and identity), enabling illegal immigration, terrorism, or espionage, obtaining medical treatment or other services, evading criminal prosecution, social security fraud, tax return fraud, residential leases fraud, securities and investments fraud, and bankruptcy fraud.

Credit card fraud is the most common type of identity theft. Most often, this type of fraud involves the thief opening a new credit card account in the victim's name; alternatively, a thief calls the credit card company of the victim, and pretending to be the victim, changes his or her address. Since bills are being sent to a new address, the victim remains unaware of the problem, often until a significant damage has been done to the person's credit profile.

The second most common type of identity theft is phone or utilities fraud. This type of identity theft occurs when a thief signs up for phone service (cell or residential) or utilities (including wireless Internet service) in the victim's name.

The third most common type of identity theft is banking and loan fraud. Bank fraud involves depository accounts and involves a thief opening an account in the victim's name and making electronic funds transfers, taking over someone's account, or writing bad checks on an account (IdentityTheft.com, 2007). Loan fraud involves a thief posing as the victim to take out a loan.

Identity theft types reported most frequently in Wisconsin in 2005 were credit card identity theft, phone or utilities fraud, and bank identity theft (Figure 1, Wisconsin Office of Privacy Protection, 2006). Percentages add up to more than 100% because some thefts resulted in more than one type of fraud.

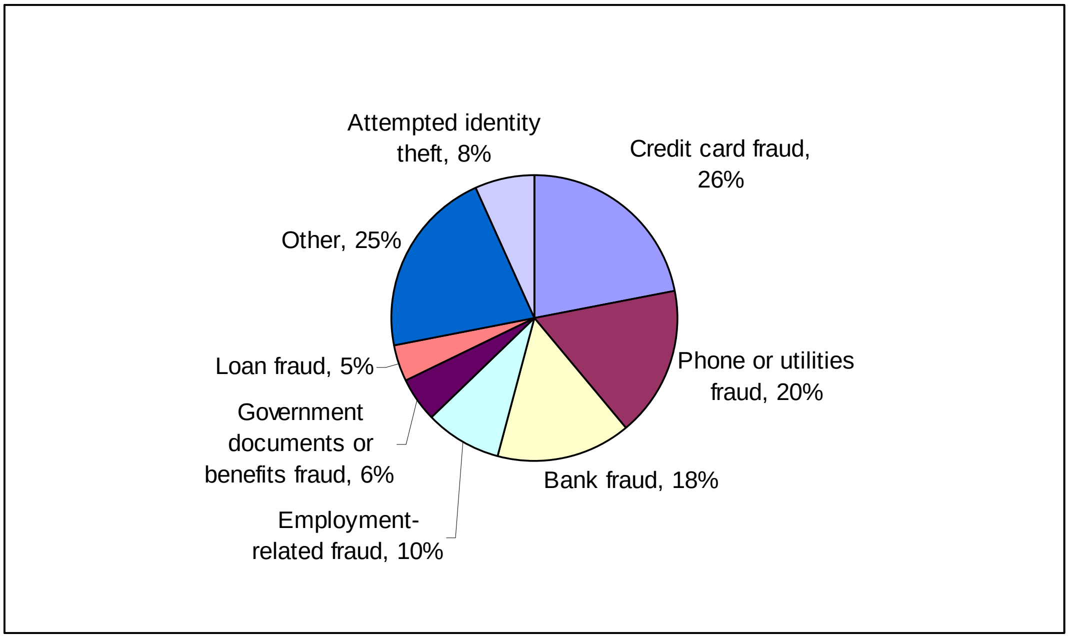

**Figure 1: Identity Theft Types Reported by Wisconsin Victims**

The main motivation for committing identity theft is usually financial gain for the thief. The motivation of financial gain most frequently coincides with credit card fraud and check fraud, bank fraud (loan and mortgage), and phone and utilities fraud.

Financial gain is not always the motivation for committing identity theft. Some thieves may commit identity theft in order to avoid prosecution for illegal activities, including illegal immigration and terrorism.

## 1.3 How Identity Theft Occurs

Identity theft can happen in many ways, including via stolen or discarded property, through phishing (described below), by thieves hacking into corporate databases, or by using social engineering to steal SPI from authorized custodians of such data.

Many kinds of private property contain SPI. A thief may steal a victim's mail or may rummage through rubbish. This most frequently occurs when an individual or a company discards documents which contain SPI without shredding or destroying them. A thief may simply steal a purse, wallet, or other objects which contains SPI. A thief may also eavesdrop on a public transaction ("shoulder surfing") in order to obtain SPI. A thief may "skim" credit card magnetic strip information, or just jot done the embossed numbers, while a card is temporarily in hand. Technological devices, such as cameras, magnetic strip readers, RFID readers, and video recorders, may aid the thieves in obtaining the information necessary for identity theft.

Laptop and desktop computers, mobile phones and personal digital assistants, and portable storage devices (including music players) can contain SPI and are theft risks. As computers have become smaller and more portable, this has become a growing area of security concern for companies that store large amounts of consumer and client SPI on their computers.

The Internet has been and continues to be an avenue for committing identity theft. Thieves use the Internet for identity fraud by hacking into corporate computers and databases that contain SPI. Spam e-mail and phishing are two other common mechanisms used for identity theft from consumers. Spam e-mails are generally advertisements that offer victims a benefit of some sort (usually false), and causes the victim to reveal some SPI in the process of performing the actions suggested in the spam e-mail. On the other hand, in a phishing attack, the thieves impersonate a trusted organization, such as a credit union, in an electronic communication that requests SPI from a victim. Phishing via voice over Internet protocol, or "vishing", is analogous to phishing, but uses voice mail and interactive voice response units instead of e-mail and Web sites as the attack vectors.

Social engineering is another misrepresentation tactic used by thieves to obtain SPI. While this kind of identity theft may occur in a face-to-face manner, today this is manifested most frequently through attacks on computer networks. Computer criminals and security consultants claim that it is actually easier to trick someone into giving up a password for a system than to spend the effort to hack in. As more and more people access and store SPI on computers and on the Internet, social engineering will become an increasingly significant attack route.

Another common mechanism for SPI loss is through the infiltration of an organization by a thief to obtain temporary or long-term access to SPI databases. The stolen data can be used directly or sold to outsiders for identity fraud. The list of pathways to SPI loss discussed in this section is by no means exhaustive – Unfortunately, perpetrators of identity theft are constantly discovering and exploiting new routes for accessing SPI from people and systems.

# 2. Areas of SPI Loss or Invasion

## 2.1 Why preventing ID theft is difficult

Currently the main way to prevent identity theft is to protect the privacy of SPI. Most organizations, including credit unions, need to store the SPI of their customers in order to provide services. Once the consumer gives his or her information to a trusted business, it is up to that organization to keep the information private.

SPI is difficult to protect. The technology needed to protect SPI with a high degree of confidence can be complex and expensive. There are many legacy systems that are difficult to update with new protection techniques. Finally, the business itself depends on fast and easy access to the SPI for optimum service, thereby creating a counter demand to privacy protection within the organization. According to a study by the Phonemon Institute, nearly two-thirds of security executives say that they have no way to prevent a breach.

Since it is difficult to fully protect SPI, the ways SPI is stolen from organizations must be examined so that effort can be focused on the most frequent and damaging problems. Alternatively, risk managers can attempt to prevent fraud by foiling attackers at a later step of the fraud process, such as during authentication.

The website Attrition.org has been tracking SPI losses by organizations reported publicly since November 2000. Additional analysis of these data can be found in Hasan and Yurcik (2006).

## 2.2 How SPI Gets Stolen

Between November 2000 and December 2006, SPI was reported compromised for at least 136,623,820 individuals across all industries. Internet hacking was responsible for 55,454,401 (41%) of SPI losses, social engineering fraud was responsible for 33,387,891 (24%), and 28,692,771 (21%) SPI compromises were from stolen computers (Figure 2).

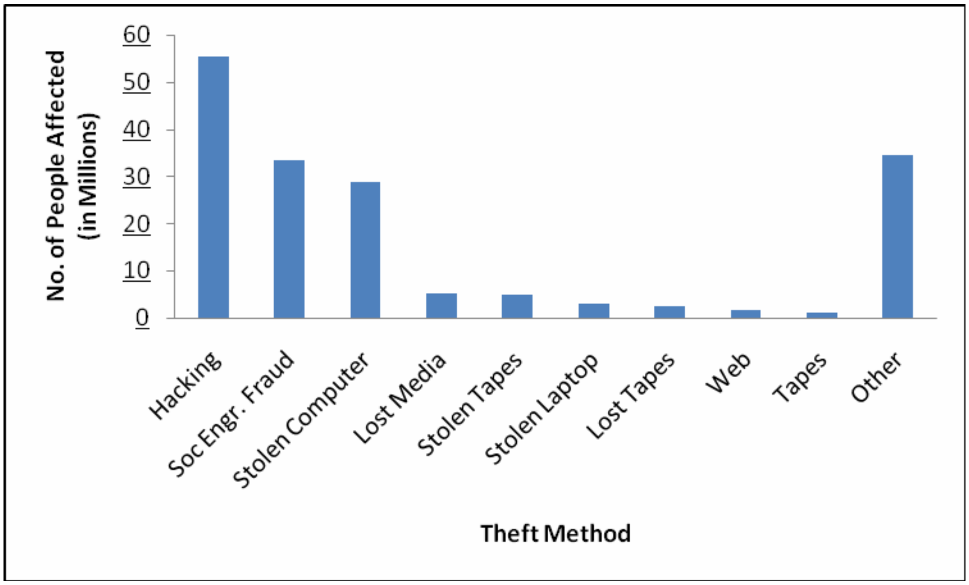

**Figure 2: Compromised Records by ID Theft Method**

If methods are ranked by the number of incidents rather than the number of records, stolen laptops and unauthorized Web access rank second and third, since many of those types of breaches involved small numbers of records (Figure 3).

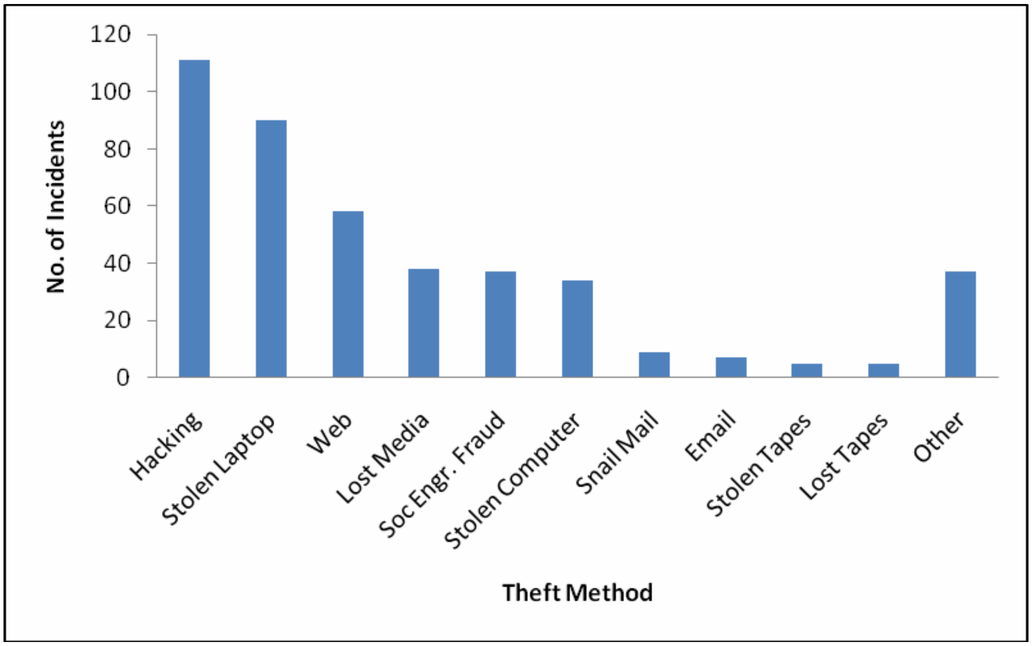

**Figure 3: Theft Incidents by Method**

Risk management officials in the credit union industry agree that credit unions serving select employee groups (SEGs) have lower fraud rates than those serving the community at large. More controls and stronger authentication of prospective members are available through employers, and affidavits can be required from employees to vouch for and accept responsibility for fraud from family members (UWEBC focus group, June 25, 2007).

Another important factor to consider concerning SPI theft is the party responsible for the theft. Between November 2000 and December 2006 and across all business types, 72% of the records stolen were from an outside source, 24% was from an inside source with malicious intent, and 4% was from an employee inside the organization who accidentally exposed SPI.

To summarize these results, the biggest area of concern for financial companies is the external threat of Internet hackers who attempt to steal credit card numbers, social security numbers, and other account numbers by breaking into systems containing such SPI.

# 3. SPI Loss That Turns Into Identity Theft

According to Computerworld (September, 2006), research has shown that less then 1% of all SPI loss incidents eventually result in identity theft. Most SPI thefts result from lost or stolen wallets or other personal property, not corporate data breaches.

A study by Javelin Strategy & Research on 217 identity theft victims who claimed to know how their SPI was stolen shows that 31% of identity theft originated from a stolen or lost wallet. Only 6% of identity theft was caused by corporate data breaches (Figure 4). This, however, does not absolve credit unions from most responsibility. Credit unions have historically and, as cooperatives, rightfully taken the responsibility to educate their members on financial matters, and security is an important and popular topic for credit union education programs.

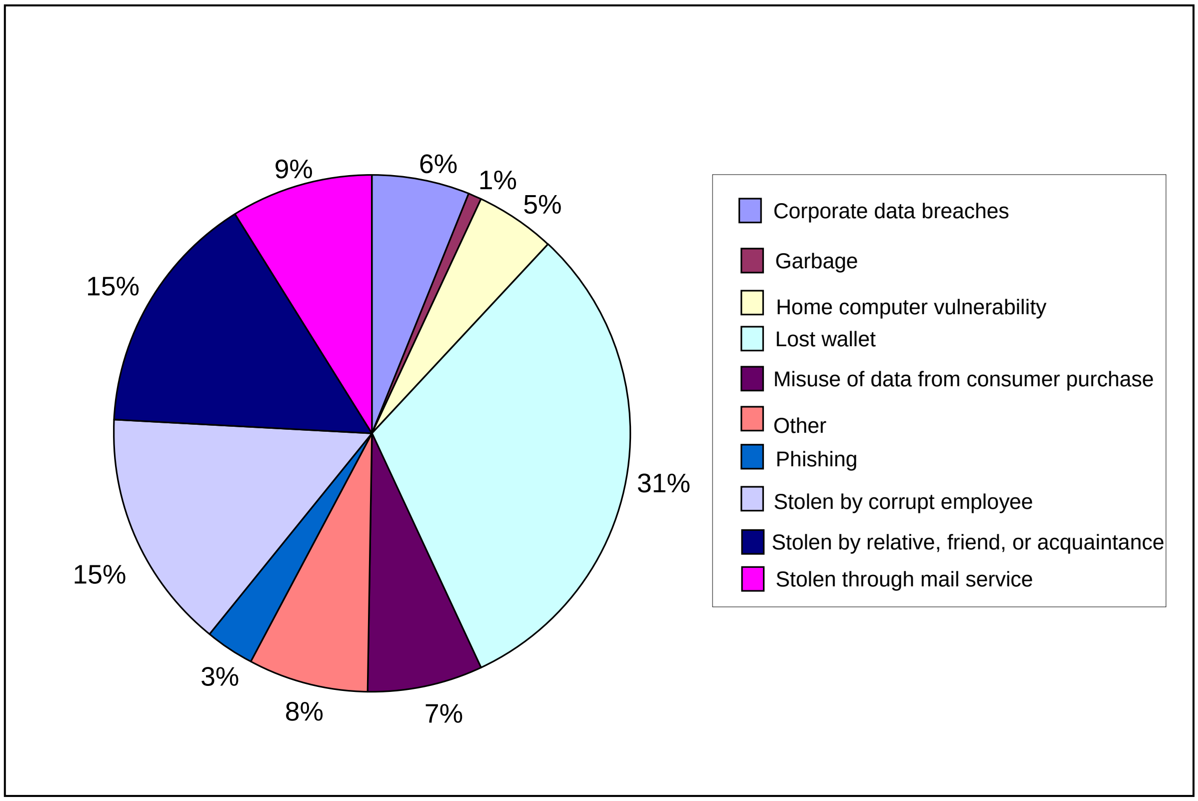

**Figure 4: Sources of ID Theft**

These findings indicate that increased SPI protection may have diminishing effects on aggregate SPI theft, because credit unions do not control all aspects of SPI custody, and thus cannot completely prevent its theft, even with extensive member education. More data should be gathered that further breaks down the SPI theft that results from corporate data breaches. There is a need to quantify the SPI that eventually became identity theft, how the SPI was stolen, what SPI was stolen, and who was responsible for the data loss. Documented cases of identity theft should be mapped to attack trees (explained next) to insure that new and novel paths leading to identity theft are addressed, if warranted, by effective countermeasures.

# 4. Attack Tree Description of ID Theft & Prevention Countermeasures

## 4.1 Attack Trees Overview

Attack trees were developed by Bruce Schneier (1999b) to serve as a formal way to document the possible sequences of events leading to an intentional but unwanted outcome (an “attack”). They are used to summarize the output of threat modeling, the systematic listing of all possible avenues by which attackers can attack some kind of asset (Hasan *et al.*, 2005). Threat modeling is the first step in security management. It is followed, in turn, by risk management, the specification of security requirements, and the development and implementation of countermeasures.

Attack trees provide a method for coming to grips with the complex constellation of security threats and possible countermeasures to a system. Attack trees can be represented graphically, or completely as text. A sample (and incomplete) attack tree illustrates the events leading to the theft of a car (Figure 5).

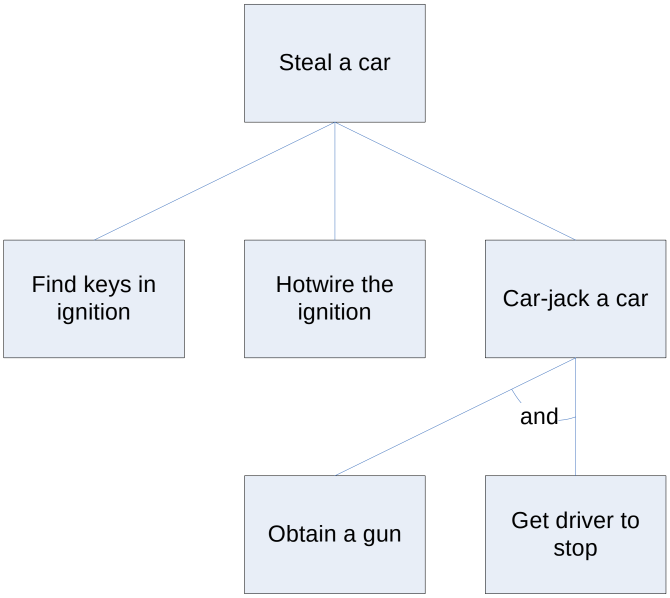

**Figure 5**

The goal of the attack is shown at the top. Possible ways to achieve the goal are shown as lower nodes in the tree. "And" arcs indicate where multiple subgoals must be met to achieve a goal at the next level.

The text representation of attack trees is more compact and better suited for representing complex situations. For example, the sample tree above can be represented by this text tree:

```
Goal:  Steal a car
1.  Find keys in ignition
2.  Hotwire the ignition
3.  Car-jack the car (AND)
    3.1  Obtain a gun
    3.2  Get driver to stop
```

Subtrees are reusable. Once a subtree like "Obtain a gun" is developed, it can be used repeatedly in multiple attack trees.

Bruce Schneier says, "In many ways, applying security measures is like sticking a tall spike in the ground and hoping that the enemy runs into it. Attack trees are a methodology to ensure that security is a broad palisade" (Schneier, 1999a).

## 4.2 Attack Trees of Identity Fraud

Identity fraud is the commission of a crime using a stolen or synthetic identity. Developing a secure identity authentication system is a countermeasure against every attack that requires identity fraud as a necessary component.

One way to treat the problem is to outline an identity fraud subtree, then identify where it can be used in a tree of attacks against credit unions and their members. An attack tree for identity fraud in the credit union context follows.

In essence, there are two main identity authentication systems for humans. One is based on the recording of a birth and the chain of custody of a baby by its parents and others, such as hospital staff, through the child's age of self-awareness. This system associates certain identifiers, particularly the child's name, parents' names (for example "David, son of Jesse"), place of birth (e.g., "Joan of Arc"), and (in modern times in the United States) a social security number (SSN), to a particular person. Recording of deaths is also part of this system. Before emergence of modern information systems in the twentieth century, identity was authenticated primarily by trusted introducers, beginning with family members and parents' neighbors who knew the person from birth.

Commerce uses a different system, one that has been called “information-based authentication” (Gordon and Willox, 2003). In this system, an adult claims identifiers (name, SSN) by providing information about the person with the identifiers that only the person identified would be likely to know: password, personal identification number (PIN), social security number, place of birth, mother’s maiden name, and so on.

Biometrics (photographs, signatures, fingerprints, iris scans, DNA profiles, and similar physical and biological attributes of an individual) can only assist in these systems, by proving that the same individual is the subject of both the foundation birth record and subsequent transactions. If the birth record is suspect, biometrics cannot improve the situation.

The two main flaws in information-based authentication are the “life story” vulnerability and the “trusted verifier” vulnerability.

In the life story attack, an attacker studies a target in detail to learn so much about the target from public records, neighbors, employers, and other sources, that, after memorization and practice, the attacker can pass virtually any information-based test of identity. While attack would not work on a public figure, such as a political leader or media celebrity, it is easy enough for an ordinary person who grew up in another region of the country and is alleged by the attacker to have just moved to the attacker’s current address. While the cost of this attack is high (months of research and study), and not justified for low-value objectives, such as fraudulently applying for a loan, the cost may be justified for high-value targets of terrorism or espionage.

The trusted verifier attack is far easier to mount. Information-based authentication requires that there be a veritable army of trustworthy agents available to authenticate the parties of every commercial transaction using SPI, information that the army must otherwise keep secret. For example, mothers’ maiden names were once widely used as passwords by financial institutions. Who knows your mother’s maiden name? In addition to all the employees of all the financial institutions you and parents have used, and the consumer credit reporting agencies, there are registrars of births, all your mother’s friends, genealogy Web sites, school systems, alumni associations, and many more.

Most of what is now called identity theft is caused by leaks of this “secret” SPI from trusted verifiers to others, a flow that is unlikely to ever be stopped, because information that is supposed to be secret when authenticating identity is essential public information in other contexts. The community of trusted verifiers is fully connected with the rest of us. Official databases, from social security numbers and drivers license records to lists of terrorists and sexual predators, cannot be compiled without errors.

Hasan *et al.* (2005) developed two procedures to systematically discover all possible threats to data, such as SPI, in storage systems. Because SPI may have long and complex life cycles, the data lifecycle threat model process may be more useful for systematically identifying emerging vulnerabilities and threats to the integrity of identification and authentication. This review has not attempted to consider all possible workflows for vulnerabilities. However, an institution should conduct such an analysis of its own processes to proactively identify threats. To the extent that practices are uniform through the credit union industry, such an analysis may be generally applicable to all credit unions.

Since attack subtrees for common components like “Authenticate using SPI” reappear at various points in a larger tree as complex as “Commit Identity Fraud”, some thought and experimentation is required to determine a tractable, much less optimal, decomposition of the tree. In programming terms, we need to determine what frequently repeated components should be implemented as subroutines.

The focus of this report is to examine how Credit Unions in the United States, and their members, can be victimized by fraud that involves identity theft. Therefore, “Obtain a fraudulent identity” appears several places in the main attack tree. Other frequently reoccurring subtrees include "Authenticate as a potential member" and "Authenticate as a member". These subtrees are full of opportunities for both fraud and its prevention.

First, the "Obtain a fraudulent identity" subtree. Countermeasures for credit union members are in **bold**. These imply credit union countermeasures to educate, enable, and encourage the member behavior. Other countermeasures for credit unions are in ***bold italics***.

Goal: Obtain a fraudulent identity that can withstand an authentication challenge (AND)
***Lobby lawmakers for action on all aspects of ID theft***
***Educate and learn from law enforcement officials about ID theft***
***Encourage and participate in state one-stop reporting programs like the Georgia Stop Identity Theft Network***
1. Obtain an additional identity
1.1 Steal sensitive personal information (SPI)
1.1.1 Steal SPI from data owner
***Educate members, the public, and SEG groups on ID theft***
***Educate members that ID theft insurance is of little value***
***Don't sell ID theft insurance***
**Don't purchase ID theft insurance**
1.1.1.1 Dumpster dive
**Shred mail and other unneeded personal papers**
***Provide shredders in lobby for member use***
***Provide home shredders as prizes or at cost***
1.1.1.2 Steal mail
1.1.1.2.1 Inbound
**Use a post office box, mail slot, or secure mailbox**
1.1.1.2.2 Outbound
**Deposit mail only in USPS deposit boxes or at post offices**
1.1.1.2.3 In transit
**Pay using on-line services or ACH instead of checks**
1.1.1.3 Steal SPI from family members ("friendly fraud")
**Keep personal papers in a locked file cabinet**
**Password-protect personal computers**
***Require affidavit from SEG employees for family members***
***Hold SEG employees responsible for family member fraud***
1.1.1.4 Steal SPI of child, inmate, or disabled dependent
1.1.1.5 Steal wallet, purse, or vehicle
**Carry the minimum necessary SPI when out**
**Keep a list of SPI carried at home**
1.1.1.6 Steal home or mobile computer, phone, PDA
**Encrypt data on portable devices**
**Keep portable devices locked up out of sight**
1.1.1.7 Phish or vish (phish over voice over IP) for SPI
**Understand the risks and don't fall for them**
***Educate members on phishing risks***
***Do not use e-mail for marketing***
***For transaction confirmations, use a consistent e-mail style and teach members to recognize it***
***Use unique login screen features for each member***
***Offer free Web site screening software to members***
1.1.1.8 Log keystrokes
**Keep computers malware-free (anti-virus, etc.)**
1.1.1.9 Eavesdrop on Internet traffic
**Use only encrypted channels like SSL for SPI**
1.1.1.10 Eavesdrop on lobby transactions

***Rope off waiting areas from teller areas***

1.1.1.11 Photograph lobby or ATM transactions

***Educate members on shoulder surfing risks***

***Prohibit cell phone use in lobby***

1.1.1.12 Obtain decedant SPI from obituaries

**Notify authorities of deaths immediately**

**Don’t publish SPI in obituaries**

1.1.1.13 Troll detailed profiles in social networking communities

**Don’t publish detailed SPI in social network profiles**

1.1.1.14 Use social engineering to obtain SPI from owner

**Learn the risks and don’t fall for them**

***Educate members on 419 and other current scams***

1.1.2 Steal SPI from data custodian

***Use PCI DSS procedures for all SPI***

1.1.2.1 Dumpster dive

***Use secure recycling containers***

***Hire screened, bonded disposal contractors***

1.1.2.2 Steal equipment or data media

***Encrypt backup media***

1.1.2.3 Hack into database

***Encrypt SPI at rest and in transit***

1.1.2.4 Compromise Web site

***Follow best practices for network and host security***

1.1.2.5 Use social engineering (e.g., pretexting)

***Educate employees on the risks of social engineering***

***Restrict access to back-office areas***

***Use strong sign in/out procedures for contractors***

1.1.3 Unauthorized use of SPI by custodian employee or contractor

***Run background and credit checks on employees***

***Vet contractor personnel as carefully as employees***

***Use the right kind of shipper for sensitive data***

1.1.4 Buy custodian’s surplus systems or media

***Render old media and hard drives unreadable before discarding***

***Use strict procedures for decommissioning systems, printers, copiers, fax machines***

1.1.5 Bribe custodian employee or contractor (outside attack)

***Watch for changed employee behavior or financial position***

***Offer rewards for the arrest of bribers***

1.1.6 Purchase stolen SPI from on the black market

***Use countermeasures to prevent the original theft of SPI***

1.2 Create a synthetic US identity (AND)

1.2.1 Fake a birth

***Require additional checks for adults with new SSNs***

1.2.1.1 Cause a fraudulent birth to be recorded

1.2.1.2 Wait eighteen or more years, generating history and public records for the nonexistent person

1.2.2 Fake a naturalization

1.2.3 Forge or steal non-US identity documentation

***Require US documentation of permanent resident status***

2. Obtain breeder documents (birth certificate, social security card, driver’s license, passport, SEG identification)

***Support strong, diverse systems for issuance of state and federal identity documents***

***Oppose one-size-fits-all systems like REALID***

2.1 Apply for breeder documents

2.1.1 Authenticate with SPI

```
  2.2  Forge breeder documents
    2.2.1  Steal and modify documents
      2.2.1.1  Steal equipment and stock
      2.2.1.2  Bribe government officials
      Support a well-paid and well-educated civil service
  2.3  Purchase breeder documents on black market

3. Apply for additional identifiers using SPI and breeder documents
(credit cards, bank accounts, merchant accounts, voter registration,
wireless telephone accounts, utility accounts) (AND)
Require a galaxy of consistent history records over adult life to
support questionable breeder documents
Verify easily forged documentation (e.g., pay stubs) with issuer
Offer copies of credit reports to members after credit checks
Respond aggressively to SPI breach reports
Obtain a free credit report from each consumer credit reporting agency
every year
Apply credit freeze to consumer credit records
Apply fraud alert to consumer credit records
  3.1  Apply for low risk credit (e.g., subscribe to magazines on line)
    3.1.1  Authenticate
      3.1.1.1  Authenticate with SPI
      3.1.1.2  Authenticate with breeder documents
```

We are now in the position to create the overall attack tree.

```
Goal:  Commit fraud against credit unions and members
Lobby lawmakers for action on all aspects of ID fraud
Educate and learn from law enforcement officials about ID fraud
1. Commit financial fraud
  1.1  Steal financial assets
    1.1.1  Steal assets of members
    Verify street address changes by mail to new and old addresses
    Verify e-mail address changes by phone or in person
      1.1.1.1  Withdraw funds from share account
        1.1.1.1.1  Pose as account owner (AND)
        Do not approve withdrawals to recent new addresses
          1.1.1.1.1.1  Authenticate as CU member
          1.1.1.1.1.2  Redirect account mailings and e-mail
          1.1.1.1.1.3  Withdraw share funds
        1.1.1.1.2  Pose as personal representative (AND)
          1.1.1.1.2.1  Forge death certificate
          Verify death with local officials
          1.1.1.1.2.2  Authenticate as personal representative
      1.1.1.2  Abscond with loan proceeds (AND)
      Do not approve loans to recent new addresses
        1.1.1.2.1  Authenticate as CU member
        1.1.1.2.2  Redirect account mailings and e-mail
        1.1.1.2.3  Withdraw loan proceeds or from revolving charge
      1.1.1.3  Pass the member's stolen checks (AND)
      Hold funds for deposits until items finally clear
      Collect thumb prints when accepting suspicious items
        1.1.1.3.1  Steal member's checks
        Sent separate notice of check shipment
        Send checks in unmarked boxes
        Establish permanent stop payment procedures
        1.1.1.3.2  Authenticate as CU member
```

1.1.1.3.3 Redirect account mailings and e-mail

1.1.1.3.4 Cash the forged, stolen checks

***Do not accept washed checks***

1.1.1.4 Make fraudulent credit card charges (AND)

1.1.1.4.1 Control existing credit card account

1.1.1.4.1.1 Steal credit card

1.1.1.4.1.2 Skim magnetic stripe data

1.1.1.4.1.3 Shoulder surf card PIN number

1.1.1.4.1.4 Redirect account mailings and e-mail

1.1.1.4.2 Make fraudulent charges

1.1.1.4.2.1 Charge in person with stolen or cloned plastic

***Verify hologram and signature***

***Verify expiration date***

***Verify magnetic stripe card validation value***

1.1.1.4.2.2 Charge by phone or on line with SPI

***Verify expiration date***

***Verify printed card validation value 2***

***Require shipping to credit card address***

1.1.1.5 Make unauthorized ATM withdrawals (AND)

1.1.1.5.1 Control existing share card account (AND)

1.1.1.5.1.1 Steal ATM card

1.1.1.5.1.2 Shoulder surf card PIN number

1.1.1.5.2 Redirect account mailings and e-mail

1.1.1.5.3 Make fraudulent withdrawals

***Verify printed card validation value 2***

1.1.2 Steal assets of credit union

***Prohibit sunglasses and hats in lobby areas***

1.1.2.1 Pass bad checks or money orders

1.1.2.1.1 Steal blank check or money order stock

1.1.2.1.2 Steal mail containing checks that can be washed

***Give extra scrutiny to Walmart money orders***

***Take thumbprint from depositors of large checks or money orders***

***Hold funds five days before withdrawals or wire transfers***

***Require service centers to use the same checks as credit unions***

1.1.2.2 Borrow money under fraudulent identity (AND)

1.1.2.2.1 Obtain false identity eligible for membership

1.1.2.2.2 Deposit cash to open a share account

***Verify employment for indirect loan origination***

***Require same authentication by indirect lenders as by employees***

1.1.2.2.3 Qualify for loan under false identity

***Require indirect loan originators to share risk***

1.1.2.2.4 Present false photo identification to pick up cash

1.1.2.3 Apply for new credit card account

1.1.2.3.1 Obtain false identity eligible for membership

1.1.2.3.1.1 Deposit cash to open a share account

1.1.2.3.1.2 Qualify for credit under false identity

1.1.2.4 Insider threats using fraudulent identity

1.2 Launder money

***Accept large amounts of cash only from members***

***Require positive identification when accepting cash***

***Verify account name as well as number matches for ACH transfers***

1.3 Pass counterfeit money

***Accept large amounts of cash only from members***

***Require positive identification when accepting cash***

***Educate employees on detecting counterfeit money***

2. Anonymously commit other crimes, e.g., arson (outside the scope of this report)

Since one of the most fruitful areas for countermeasures is the authentication of new members and members receiving financial benefits (e.g., loan proceeds), it is useful to provide subtrees for these authentication processes.

Goal:  Authenticate as person eligible for CU membership (AND)
1. Obtain a fraudulent identity in the community or SEG
***Verify employment with employer***
2. Pass the CU's authentication tests for enrollment
***Use an unpredictable variety of identity checks***
***Require state-issued photo identification***
***Require additional documentation if application data cannot be verified***
***Scan and validate machine-readable data on photo ID***
***Verify date of birth, past addresses (e.g., LexusNexis Accurint)***
***Match application data with credit verification report (CVR)***
***Open youth accounts only for the dependents of members***
***At initial branch visit, collect biometric data (photograph, signature, thumb print) and store on network***

Goal:  Authenticate as CU member (AND)
1. Obtain the member's fraudulent identity
2. Pass the CU's authentication tests for a transaction
***Use an unpredictable variety of identity checks***
***Require state-issued photo identification***
***Scan and validate machine-readable data on photo ID***
***Verify death of decedent with officials before providing asset access to a personal representative***
***Require new members to establish a password for phone or on line access***
***Provide no financial benefits before collecting biometric data***
***When providing financial benefits, verify biometric data***
***Verify photograph with employer or school official***

# 5. Strategies for Combating Identity Theft

Attack trees provide a convenient and rigorous method for quantifying the cost and effectiveness of security measures.  Countermeasures can be assigned to nodes, along with costs, probabilities of success, and estimates of other parameters (e.g., cost of special equipment, time required, special expertise required).  Assumptions about attack steps can be made explicit, and if necessary, new nodes in the tree can be added to illustrate them.

Often analysis of a node will reveal other vulnerabilities, assumptions, errors of logic, and so on. The attack tree can then be reorganized or elaborated to accommodate the new knowledge. Questions like "How could a person get a new social security number?" allow the analysis of systems like the ones intended to prevent the issuance of duplicate SSNs.

In the credit union context, there are two main strategies for preventing identity fraud:  rigorous authentication at the points of establishing membership and providing financial benefits, and education of customers and the public to help them protect themselves.  Given below are the top recommendations for authentication countermeasures.

## Authentication Countermeasures at the Point of Establishing Membership

1. Require state or federal photo identification documents to become a member: driver's license, state-issued non-driver's identification, passport.
2. Check documentation for indications of tampering or forgery. Collect and interpret any machine readable data in the documents and compare to face of document and application.
3. Verify with officials the employment of adults and school attendance of minors.
4. Run a credit verification report on each adult applicant.
5. Use a name and address validation service for initial screening.
6. Cross-check SPI between that offered by the applicant and official sources.
7. Require explanation and additional documentation if documents do not match database records: court order of name change, utility bills, letter of reference, etc.
8. Collect biometric information during the new member's first in-person visit: scanned signature, photograph, thumbprint. Store biometric information on the CU network. Verify with employer or school officials the photograph of new member.
9. Require the new member to select a password for on-line and telephone transactions.
10. Require that the parents or guardians of new youth members also be members.

## Authentication Countermeasures at the Point of Providing Financial Benefits

1. Require a waiting period before new members are eligible for loans.
2. Require a waiting period before members may convert checks to cash.
3. Use credit monitoring services to spot deviations from normal charging behavior.
4. Use an on-line check validation service to monitor stolen, counterfeit, or washed checks.
5. Require both account number and owner name to match for ACH transfers.
6. Verify with officials the death of a member before providing account access to a personal representative.

It is the authors' hope that credit union professionals will carefully review the attack trees outlined above to discover countermeasures that they can add to their credit union's procedures, as well as any omitted attack paths that should be documented and shared, and new countermeasures. Over time, additional experience should permit the countermeasures listed above to be ranked in value and cost-effectiveness. Finally, security from identity fraud is a never-ending race, with new threats and new countermeasures emerging all the time. Credit union risk management teams should review the attack trees above, or versions customized for their situation, whenever new threats are discovered or new countermeasures devised, but no less often than annually.

# 6. References

Arnold, Tom, June 2000. CyberSource Corporation, “Internet Identity Theft ’A Tragedy of Victims’”.

Attrition.org, 2007. Data Loss Archive and Database http://attrition.org/dataloss/.

Better Business Bureau, 2007. http://www.bbbonline.org/IDtheft/.

Gordon, Gary R, and Norman A Willox, Jr., 2003. Identity fraud: a critical national and global threat, Economic Crime Institute, Utica College, Utica, NY, 48 pp.

Hasan, Ragib, and William Yurcik, 2006. A statistical analysis of disclosed storage security breaches, Proceedings of the Second ACM Workshop on Storage Security and Survivability, http://portal.acm.org/citation.cfm?id=1179559.1179561

Hasan, Rajib, Suvda Myagmar, Adam J Lee, and William Yurcik, 2005. Toward a threat model for storage systems, StorageSS’05, http://portal.acm.org/citation.cfm?id=1103795

Identity Theft Resource Center, 2007. http://www.idtheftcenter.org/.

IdentityTheft.com, 2007. http://identitytheft.com.

Privacy Rights Clearinghouse, September 2007. http://www.privacyrights.org/ar/idtheftsurveys.htm.

*Sarbanes-Oxley Compliance Journal*, September 2006. Two-Thirds of Security Personnel Surveyed Say They Cannot Prevent a Data Breach.

Schneier. Bruce, 1999a. Attack Trees, http://www.cs.utk.edu/~dunigan/cs594-cns96/attacktrees.pdf.

Schneier, Bruce, December 1999b. Attack Trees: Modeling Security Threats, *Dr. Dobbs Journal,* http://www.schneier.com/paper-attacktrees-ddj-ft.html.

U.S. Department of Justice, September 2006. Fact Sheet: The Work of the President’s Identity Theft Task Force.

Vijayan, Jaikumar, September 2006. Data Breaches Yield Few ID Thefts, *ComputerWorld.*

Wells, Susan J, December 2002. Stolen Identity, *HR Magazine.*

Wikipedia, September 2006. http://en.wikipedia.org/wiki/Identity_theft.

Wisconsin Office of Privacy Protection. 2007. http://privacy.wi.gov/.