Liberty Alliance Whitepaper: Identity Theft Primer

December 5, 2005

Overview

Many decades ago, a reporter asked the infamous thief Willy Sutton why he robbed banks. Sutton's reply is reputed to have been "Because that's where the money is."

Today, money is in information, and there is a lot of information out there, much of it vulnerable in databases, exposed in transactions and circulating on the Web. In today's black market, Social Security numbers, home addresses, credit card numbers and other pieces of data represent "where the money is," making identity theft the fastest growing crime in the world.

From the criminal's point of view identity theft offers an excellent business proposition: it's easy to do, it's difficult to track and prosecute and there's an opportunity to make a great deal of money.

And identity thieves are doing well. Losses to business and financial institutions over the course of 2003 amounted to nearly $48 billion, with consumer victims reporting an additional $5 billion in out-of-pocket expenses.

All over the world, governments, trade groups, individuals and corporations are trying to identify how to beat this escalating threat. Identity theft is a crime which spans the boundaries of organizations, companies and countries. No 'single-enterprise' solution can ever address the problem satisfactorily. Because the potential for damage is so diversified, it is critically important that resources are pooled and joint solutions are developed.

The authors of this paper represent the Special Interest Group (SIG) on Identity Theft within the Liberty Alliance, a global consortium for open federated identity standards and identity-based Web services. Liberty itself represents more than 150 leading banks, telecommunications companies, service providers, vendors and government agencies around the world. The group has investigated the topic of identity theft in detail, and presents its findings in this white paper, clearly explaining how a cross-organizational and vendor-neutral method of approaching the problem can work where piecemeal approaches will not.

It is worth explicitly noting that because at present a majority of identity theft occurs in the US, this whitepaper takes a distinct US-centric focus. However, we are conscious that identity theft is a growing crime internationally, and thus we try to address the related global issues as well as well those that are US-centric in nature.

Audience

This white paper is intended for both business and technical readers who want to gain an overall understanding of identity theft, its causes and impact. It presents the Identity Theft Lifecycle, and explains how stolen identities are converted into money. Companion white papers explore the related topics of how data custodians, technologists and businesses can help stop identity theft.

Identity Theft – What it is, and why it matters

1. Identity Theft Defined

Confusion exists in the minds of consumers, financial institutions and even policymakers as to exactly what is meant by “identity theft”. The United States Federal Trade Commission (FTC) defines identity theft as 'a fraud that is committed or attempted, using a person’s identifying information without authority'. This broad definition came out of 1998 legislation designed to provide consumer protections against the fraudulent use of personal information in any form **Identity Theft and Assumption Deterrence Act of 1998**, Title 18 United States Code – Section 1028.

Financial institutions vary in their definitions of the term, and closely couple the definition with the type of fraud in question. Credit card companies use a narrow definition of identity theft, and have developed different approaches to managing fraud committed with a lost or stolen credit card, and the more complex fraud that occurs when someone’s identity is used to fraudulently establish new accounts. While there is no legal distinction between the two types of fraud, the risk to individuals is quite different. The banking industry, on the other hand, uses very different detection and prevention tools in dealing with these two types of fraud and applies the term “identity theft” only to refer to the latter, more-difficult-to-detect form of identity fraud.

Many financial institutions are insisting on the following definition of identity theft: “Using someone’s personal information to obtain *new* accounts in that person’s name.” Unfortunately, this sidesteps the situation where a criminal uses personal information to drain someone’s account. That is considered account fraud, not identity theft. Account fraud is often the goal of phishing scams, an increasingly common identity theft technique. In the minds of the consumer and the media, identity theft and fraud are often interchangeable.

2. Categories of Identity Theft

The Liberty Alliance categorizes identity theft in three ways, based on the uses to which the thief puts the stolen information:

- **'True name' identity theft** occurs when the thief obtains personal information and uses it to open new accounts. The thief might open a new credit card account, establish cellular phone service or open a new checking account in order to obtain blank checks.

- **Account takeover** describes the situation where an impostor steals personal information and uses it to gain access to the victim’s existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem.

- **Criminal identity theft** occurs when a criminal steals and then gives another person’s identifying information in place of his or her own to law enforcement. This could create a criminal record or leave outstanding arrest warrants for the person whose identity has been stolen.

3. Impact of Identity Theft

Identity theft's impact is seismic: it damages business and individuals, and erodes trust in the digital ecosystem and raises the cost of living.

On the consumer side, the situation is particularly disheartening as thousands of individuals are stripped of their good credit and reputation and forced to spend time, money and emotional capital on getting their lives back in order. The authorities are often ill-equipped to help consumers pursue justice due to jurisdictional issues as well as the number of cases being pursued, especially since identity theft thrives in a distributed environment (as will be seen later in the Identity Theft Lifecycle).

The statistics speak for themselves:

- Identity theft costs consumers $5 billion annually in out-of-pocket costs.
- 27.3 million Americans have been victims of identity theft in the last five years
- On the average, 49% of all victims do not know how their information was obtained.
- Nearly 85 percent of all victims find out about their identity theft case in a negative manner, whereas only15% find out due to a proactive action taken by a business.
- Victims typically spend 600 hours repairing the problem.
- The emotional impact of identity theft has been found to parallel that of victims of violent crimes.

Source: Identity Theft Resource Center (ITRC) http://idtheftcenter.org/facts.shtml

Identity theft also takes a severe toll on business. The FTC reports that in 2004, identity theft losses to business and financial institutions totaled $47.6 billion. Identity theft also impacts the following areas:

- **Brand damage**. This is particularly evident in phishing attacks when identity thieves impersonate trusted organizations, creating false emails and Web sites to steal personal information. Credibility suffers whenever a breach is reported.
- **Costly customer account repair**. Corporations that issue credit to people they believe are good credit risks, but are actually criminals, typically bear the cost of credit extended.
- **Systems failure**. In cases where a computer system is breached, organizations have to bear significant costs in shoring up the security features of those systems so that they are not breached again
- **Legal costs**. Companies and consumers who are damaged by breaches are increasingly turning to private legal action to try to gain compensation for those losses. While there is little or no established precedent to determine how successful such cases will be, even the cost of simply fending off such lawsuits may become significant.

Merchants Bear Serious Costs (SIDEBAR)

Merchants represent a special subset of organizations impacted by identity theft and fraud, and they are struggling with how to respond to identity theft and credit card fraud. It is estimated that merchants "eat" $1.5 to $3 billion annually with this figure climbing steadily as online sales continue to increase.

Under standard Visa and MasterCard rules, if the fraudulent transaction was made in person, the merchant is usually not liable for the loss. If, however, the transaction was made online or over the phone in what is known as "Card Not Present"

transactions, duped retailers lose out in multiple ways: they lose the merchandise if it is never recovered; they lose the money they paid to process and ship the items; the payment for the merchandise is reversed; and they often pay a fee to the credit card company when the chargeback is made.

The Merchant Risk Council, a nonprofit organization representing online merchants, vendors, financial institutions and law enforcement agencies, reports that while their members are fighting back with fraud prevention tools and strategies to meet this rapidly evolving threat, fully 60 percent of the merchants polled believed that
Source: Press release on Market Wire 02/03/2004 www.merchantriskcouncil.org.

Identity Theft – How it Works

1. The Identity Theft Lifecycle

Identity theft always involves an individual or group obtaining key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise and services in the name of the victim, or to provide the thief with false credentials.

Identity theft is usually a two or three-part crime: information about identities is stolen, and then the information is either used directly, or sold on the black market to others who use it, to illegally make purchases or access funds. The key element to all identity theft is *access* to personally identifiable information. There are often additional significant preparatory phases, as well as multiple monetization phases, and these may be committed by multiple individuals acting in loose cooperation. In terms of threat analysis, it would be a mistake to think of Identity Theft as an *ad hoc*, opportunistic or 'casual' crime. There is abundant motivation for Identity Theft to be used as a tool for organized crime – both for direct financial gain and also as a way of establishing false identities to further other criminal activities.

In fact, the identity theft lifecycle can easily be seen to encompass six major phases, each with multiple steps. See the following illustration for an overview of the various phases and steps within each phase.

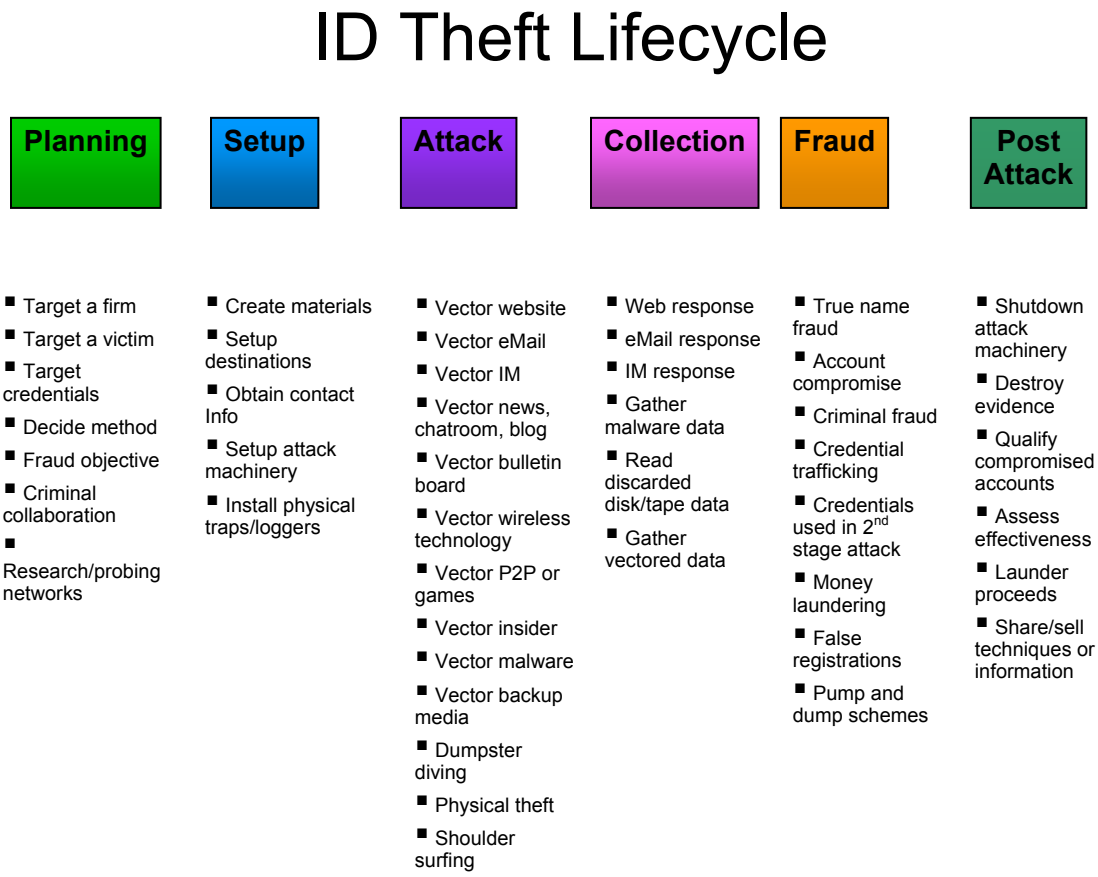

Figure 1 – Identity Theft Lifecycle

2. Attack Vectors

Identity thieves work in a wide variety of ways, both online and offline, to acquire the information they need in order to actually make money. We call these methods **attack vectors,** a term that refers to the routes or methods used to invade computer systems. In an attack, the goals are often (but not limited to) money disbursement via: EFT, wire transfer, line of credit, check, credit/debit card, bill pay, scheduled automatic withdrawals, loans (including mortgages) and funds transfer between accounts.

An understanding of the objective of the attacker (think back to the IDTheft Lifecycle phases) helps to explain potential mitigating controls that can be put into place. The table below summarizes, at a high level, the various types of attacks, providing definitions: You will note that there are three different types of attack vector. Some are technical, and exploit computers and Internet connections. Others are physical, and involved such low-tech activities as snooping through the rubbish (often referred to as “dumpster diving” from the American term for a refuse skip). Still others rely on “social engineering”, a common attack taking advantage of human nature to gain personal information.

The tables presented below contain a wealth of information on all three types of attacks, the objectives of each, a brief description, and the mitigating measures that might be taken to thwart them. Note that much of the information in the tables is cryptic for the sake of brevity, but full definitions of the attack vectors can be found in the Glossary which accompanies this document. Descriptions of the mitigating factors are presented in the Glossary as well.

Objective	Type	Attack	Description	Mitigations†
Obtain Individual Identity	**Technical**	Trojan/Keystroke Logger	Spyware/Malware placed via hacking, as payload in a virus or worm, or from Web sites	**Multi-factor authentication, anti-virus. Anti-spyware**
		Wireless Intercept	Wardriving, open access points, airsnarfing. "Evil Twin" attack	**Encryption, secure configuration**
		Pharming	DNS spoofing, DNS cache poisoning, proxy attacks	**SSL/TLS**
		Scrape Web site	Gather personal data from Web sites, Web searches to use as verifiers	
		Sniffing	Collect targeted network packets	**Encrypted payload, SSL/TLS**
	Physical	Theft	Stolen laptops, purses/wallets, mail	**User education, encryption, secure configuration**
		Shoulder Surfing	Direct observation of personal information	**User education**
		Dumpster Diving	Gather discarded documents, hardware (disks)	**User education, shredding**
		Trusted Insiders	Identity information misused by individuals with access	**Encryption, need-to-know, access controls**
	Social Engineering	Phishing	Luring individuals to reveal confidential data	**Multi-factor authentication, browser toolbars**
		Family members	Identity data misused by family members	**User education**
		Legal Sources of Identity	Obtain identity data from credit bureaus, govt. agencies fraudulently	**Multi-factor authentication, user education**
		419 scams	Obtain money and/or account information	**User education**
		Trusted Insiders	Gain identity information from service providers (doctors, dentists, lawyers, etc.)	**Multi-factor authentication, user education**

Table 1 – Attack Vectors Designed to Obtain an Individual Identity

Objective	Type	Attack	Description	Mitigations†
Obtain Multiple Identities	Technical	Hacking	Gain privileged access to machines for further attacks and/or data harvesting	**Access controls, n-tier architecture, real-time monitoring, honeypots, HIPS, NIDS, firewall**
		Data attacks	SQL Injection, XSS	**Server side validation, secure coding, encrypted payload**
		Database attacks	Login attacks, inference attacks, SQL scanners	**Multi-factor authentication, encryption, HIPS**
		Password cracking	Acquire admin passwords to servers	**Multi-factor authentication, HIPS**
	Physical	Theft or Loss	Backup data, tapes, disks, laptops, etc	**Encryption, encrypted payload, policy enforcement**
		Breach firewall(s)	Connect to internal network(s)	**HIPS. NIDS**
		Dumpster Diving	Obtain discarded documents, disks, systems, etc.	**Shredding**
	Social Engineering	Gain access	To computer rooms, wiring closets, switches, routers	**Multi-factor authentication, user education**
		Trusted insiders	DBAs, employees, contractors, individuals w/access	**Multi-factor authentication, user education separation of duties, audit controls**
		Phone requests	Gain confidential information to facilitate hacking	**User education**

Table 2 – Attack Vectors Designed to Obtain Multiple Identities

3. How Information Becomes Money

As with the data theft phases of identity theft, the monetization phases can either be entirely online, entirely offline or a combination thereof. And, as has been noted previously, because of the existence of black markets which allow information to be traded easily, the actors in the monetization phase can be entirely different from those in the data acquisition phase.

Establishing credit: Criminals can establish credit using the identity of the victim, whether to purchase goods such as a car, or establish a line of credit from which funds can be directly extracted.

Draining an account: In this case, the criminals simply use the information they have gained to directly extract money from accounts, either by check fraud or by wire transfer.

Purchasing goods (generally "real world", but it can also be on-line). This involves purchasing goods using either stolen account access, or new accounts opened by the criminal.

Selling / fencing goods: in general the majority of stolen goods will be fenced – often for only 10% of their retail value.

Committing credit card fraud: While conceptually just a combination of Purchasing Goods / Selling Goods, credit card fraud is different in that the credit card companies have relatively sophisticated fraud detection algorithms, and consumers generally are not liable for fraudulent charges.

Harming one's reputation: This is often associated with eBay, as the largest online auction site. Typically, the user-ID and password of a well-known and well-trusted retailer is stolen. That account is then utilized to advertise nonexistent merchandise at attractive prices; customers send money to the fraudster and no goods are ever shipped to them. The actual retailer is then overwhelmed by angry customers, often abandoning the market altogether.

Identity Theft – Why We Are Vulnerable

1. Reasons for Vulnerability

Identity theft is a growing problem around the world, but nowhere is it as prevalent as in the United States where it is estimated that every 79 seconds an identity is stolen. There are many reasons for the increasing vulnerability. Keep in mind the identity theft lifecycle to understand just why this information is vulnerable at each phase.

Identity Theft Thrives in a Distributed Environment. Everyone's digital identity is distributed in pieces and fragments - maintained by government entities, credit card companies, cell phone providers, hospitals and other organizations. What makes identity theft and fraud so enticing and pervasive is the increasing speed with which the identity criminal can move through a distributed set of networks, and the uncoordinated way in which those attacked are forced to respond.

Large Databases with Private Information: Some companies, often known as data brokers, collect very large amounts of data on consumers. Because these companies generally do not have direct relationships with the consumers, it is very difficult for consumers to control how their data is used. Privacy laws in Europe and other areas outside the United States substantially constrain the behavior of such businesses there, limiting data sharing and preventing businesses from selling personal information.

Social Security Numbers are Everywhere: One cause of vulnerability that is almost exclusively limited to the United States is the ubiquity of an individual's social security number (SSN), which represents the "keys to the kingdom." Insurance companies regularly use them as a common identifier, as do universities. Some service providers use the SSN as the default identifier when setting up new accounts, for example for telecommunications and utilities. Armed with just an SSN, an identity theft can do a great deal of damage.

Flaws in Enterprise Security: Some organizations take a piecemeal approach to security, either failing to appreciate the implications of Internet access, database security and the mobile workforce, or recognizing the risk but giving it insufficient priority. As a consequence, they often find their systems breached.

Tension between Product Features and Security: Competitive pressures and profit often drive software developers and their hard-driving management to prize new competitive product features over properly addressing tedious, delay-ridden security requirements. This is finally changing, as top management heeds the market's refusal to accept security-poor products. A security-aware, educated and properly resourced development culture is taking root, and should be encouraged. Attacks and vulnerabilities enabled by product features should be assessed early on, upfront, carefully paying attention to and addressing threats and vulnerabilities throughout the product lifecycle.

Lax Personal Security Practices: Many households have PCs with Internet access. Unfortunately, very few individuals appreciate the concomitant risk of leaving a PC permanently attached to the Internet, or how to mitigate that risk. Surprisingly few understand the value of applying security patches, let alone how to do so. This leaves many individuals vulnerable to having their PCs remotely taken over by attackers, and it is estimated that hundreds of thousands of them have actually suffered this fate.

Expansion of Electronic Payment Systems: Today, electronic banking and bill-pay services are becoming commonplace, and formerly-wholesale automated clearing house (ACH) payments have become a vehicle for retail payments. New forms of ACH transactions, such as Internet-authorized payments, debits authorized over the telephone, and check-to-ACH conversions at the point of purchase, have produced greater opportunities for electronic fraud. Since the ACH system was largely designed with trusted endpoints in mind, it is an excellent mechanism for criminals, as it can take days or even weeks before a fraudulent account access is uncovered.

Lack of Incentive to Protect Data: Bruce Schneier, security expert, author and CEO of Counterpane wrote in the *New York Times* that **"**Personal privacy and identity theft are security problems, but they're problems of motivation, not security technology. The companies that have our data aren't motivated to protect us better because they aren't bearing the costs of not securing that data. Privacy violations make us the victims, not them. Identity theft costs us much more money than it costs them. Right now, the business incentives are for companies to collect as much personal info as they can." (*New York Times*, June 23, 2005) Apart from post-fact breach notification requirements, there are essentially no requirements in US-based non-regulated businesses (i.e. outside financial services and healthcare) to place any significant information security controls around personal information.

Identity Theft – What We Can Do About It

Identity theft, as we have shown, is a complex topic: the lifecycle is long and involved, there are multiple attack vectors that comprise electronic, physical and social approaches, and the cast of characters is quite large. The Identity Theft SIG at the Liberty Alliance has studied this issue in depth , and has compiled a series of recommendations for those parties most involved, and most capable of thwarting, identity theft.

The technology, operational and policy-related aspects of identity theft (and identity management) are closely linked to one another. Liberty Alliance's approach, which has proven popular with members and adopters, has been to ensure that its technical specifications are supplemented by guidance on implementation and best practice. Examples of this (are available on the Liberty website (www.projectliberty.org), and include privacy and security best practices, deployment guidelines, benefits of federation in a government environment and a host of other resources. Whitepapers can be found at http://www.projectliberty.org/about/whitepapers.php and other guidelines are available at http://www.projectliberty.org/resources/guidelines.php. There are also a host of case studies as well as materials provided by our membership

To produce these materials, the Alliance draws on the industry and public sector expertise of its membership. Based on input from these stakeholders, we can identify a spectrum of influencing factors which apply to identity federation projects, and many of which have a bearing on the specific area of Identity Theft. As noted above, these can usefully be categorized into technical, operational and policy-related topics.

Broadly speaking, these three categories map onto specific implementation controls as follows:

- Technical – open specifications and standards
- Operational – contracts and best practices
- Policy – legal and regulatory compliance

Each of these areas is addressed in some depth through related documents aimed at the data custodians, policy-makers and technologists.

1. Data Custodians

It is clear that data custodians - those organizations and individuals that actually receive, communicate and store personally identifiable information – are faced with many situations in which such sensitive information could be vulnerable. At the same time, data custodians have multiple opportunities to implement safeguards, adopt industry best practices and devise new methods of preventing identity theft. The Identity Protection Group within the Liberty Alliance has compiled industry best practices for reducing identity theft. See the IDTheft SIG companion document, **The Data Custodian's Guide to Stopping Identity Theft**, for specific recommendations and best practices.

2. Policy-makers

Policy-makers are in the unique position of determining how entire markets will set the baseline for acceptable privacy practices, and develop requirements for products and services that can help protect identity information. Of course, different industries and different countries place varying degrees of emphasis on policy-making as a control, ranging from minimalist (leaving industries to define and apply self-regulatory best practice) to more prescriptive approaches. It is thus impossible to draft a single set of recommendations which would apply equally to all sectors in all countries. Our companion document, **The Policy-Maker's Guide to Stopping Identity Theft**, offers a high-level summary of applicable legislation in a number of countries, so that implementers can either see what laws affect their case, or what areas of legal control look into in their own country when formulating a compliance plan.

3. Technologists

Technologists within organizations play a very key role in protecting privacy and helping prevent identity theft. Clearly, architects, software designers and software procurers are not statutorily or financially responsible for protecting personally identifiable information or preventing identity theft. Nevertheless, effective enterprise measures would include ensuring that all relevant stakeholders are included in discussions regarding solutions that could affect personal information. See the ID Theft SIG document, **The Technologist's Guide to Stopping Identity Theft**, for specific recommendations and best practices

About the Liberty Alliance and the Identity Protection Group

The Liberty Alliance Project is an alliance of more than 150 companies, nonprofit and government organizations from around the globe. The consortium is committed to developing an open standard for federated network identity that supports all current and emerging network devices. Federated identity offers businesses, governments, employees and consumers a more convenient and secure way to control identity information in today's digital economy, and is a key component in driving the use of e-commerce and personalized data services, as well as Web-based services. Membership is open to all commercial and noncommercial organizations.

Liberty has been at the forefront of next-generation Web security, having developed and deployed open specifications for federated identity management and identity-based Web services.