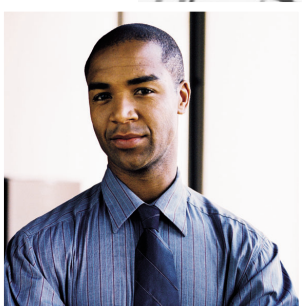


# The Merchant Supply Chain

Dangers, Challenges, and Solutions



## CONTENTS

Introduction	3
The Dangers Posed by Identity Theft	3
The Challenges Posed by Identity Theft	6
Solutions to Remedy Identity Theft	7
FOR THE MERCHANT	7
FOR THE CONSUMER	10
Conclusion	11
VISA CASE STUDY	11

## Introduction

Identity theft and credit card fraud are serious consumer issues today, representing frightening consequences and staggering costs to both business and consumers in quantifiable and non-quantifiable amounts. The Federal Trade Commission (FTC) reports that cases of identity theft have risen 177 percent in the past two years. A recently released study by the FTC indicated that in the past 12 months, 3.23 million consumers or 1.5 percent of the population discovered some form of identity theft activity.

Identity theft occurs when a person steals information that allows him or her to assume another person's identity. There are generally considered two main types of identity theft, "account takeover" and "true name fraud." Account takeover occurs when a thief acquires existing credit information and purchases products or services masked as the account holder. True name fraud or application fraud occurs when the thief uses a person's identifier such as a Social Security Number (SSN) and other identifying information to create new accounts in that person's name. Victims of true name fraud are often unaware of the crime because the individual will have used a different billing address. In contrast, account takeover victims will learn of the problem with the arrival of their monthly statements. Both types of theft carry with them startling statistics and daunting challenges for the victimized consumer and the businesses that try to guard against theft of any kind.

## The Dangers Posed by Identity Theft

The ease by which one person can assume the identity of another for fraudulent and nefarious purposes presents the real danger of this issue. The technology that has greatly enhanced aspects of daily life has also provided multiple avenues for abuse and error. Incidents of electronic fraud have multiplied exponentially with the growth of the Internet. Today, anyone who uses e-commerce systems is susceptible to having their personal information compromised. By exploiting networks, servers, and data storage devices, hackers can gain access to confidential information consumers believe is safe when conducting transactions online. Skilled identity thieves have literally hundreds of ways in which to steal information. Low-tech methods such as stealing printed records, mail, or trash can be as effective as skilled technological methods like hacking.

The danger to the consumer is that identity theft can result in loss of credit, the inability to rent or own a home, criminal charges, or employment difficulty. Identity thieves may make unauthorized purchases of big ticket items for quick resale, open wireless or phone service accounts, obtain auto loans, open new credit card accounts, or file for bankruptcy to avoid debts or eviction. A person can also use a stolen identity in the case of an arrest leaving the consumer with the possibility of outstanding warrants. In short, it can wreak havoc on a consumer's life in both immediate and long-term ways. Since theft may go unnoticed by a consumer for a period of time, and because some thieves continue to engage in fraudulent activity, the crime of identity theft is often a long-term issue that may take years to resolve.

When an identity thief targets a consumer for criminal activity to make unauthorized purchases, the individual consumer is placed at financial risk. However, when a consumer is targeted for identity theft to carry out terrorist activity, it poses a threat to the general public. At a Senate hearing held September 9, 2003, master counterfeiter Youssef Hmimssa explained how, armed with a simple laser printer, he created and distributed fake visas and other identification documents to a suspected terror cell in Detroit, Michigan, days after September 11, 2001. Hmimssa was even able to produce special ink for birth certificates that would stand up to ultraviolet light tests. Hmimssa has since confessed to fraud and is now a key government witness; his testimony helped the government earn one of its first terrorism convictions.

Once pertinent information is gained, stealing a person's identity is relatively easy. A General Accounting Office report released at the hearing indicated that undercover agents had little trouble securing driver's licenses when they produced fake documents such as birth certificates and SSN cards. The fear is that this information is also in the minds of terrorists. By using fake driver's licenses, terrorists can open bank accounts, board airplanes, and purchase supplies to move freely about the country.

Identity theft impacts businesses as well through loss of credibility, brand and customer base. And, when the perpetrator is also a current or former employee, the effects can be especially damaging. One of the most notable examples involved Acxiom, one of the world's largest specialists in customer and information management. They were forced to admit that they had been hacked, and that information about some customers of its clients was downloaded. An Acxiom spokesperson stated, "An individual, who was a former employee of an Acxiom client, was arrested in conjunction with this incident ... according to law enforcement, the individual arrested was a known sophisticated hacker. He evidently gained access through hacking of encrypted passwords."

The breach involved one external FTP server outside Acxiom's firewall that is used to transfer files back and forth between Acxiom and its clients. At the time, the company stated that no internal databases were accessed and no breach penetrated its firewall. But Acxiom, which prides itself as a leader on consumer privacy issues, landed in the middle of a media maelstrom.

Companies may also lose credibility if a scam is perpetuated in its name. Some scams will involve an e-mail claiming that there is a problem with the consumer's account or an order has been mistakenly placed which the consumer needs to cancel. The e-mail will provide a link that will take the consumer to a Web site resembling the true homepage of the company with a plausible sounding URL. The consumer will then be asked to input personal information which can range from credit card to bank account numbers and/or Personal Identification Numbers to SSNs. The information is then gleaned for theft.

Another scam gaining ground is on the use of employment sites. Popular press has reported on stories of resume rip offs where a vast number of resumes are downloaded from a site and then sold at a profit to the appropriate industry sector. In another instance, a job seeker is notified that the company has an older version of their resume and is asked to update and provide new information such as their SSN when in fact the earlier resume never existed.

**The Act makes it a federal crime when someone:**

*“Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”*

Under the Act, a name or SSN is considered a “means of identification.” So is a credit card number, cellular telephone electronic serial number, or any other piece of information that may be used alone or in conjunction with other information to identify a specific individual.

In most instances, a conviction for identity theft carries a maximum of 15-years imprisonment, a fine as well as forfeiture of any personal property used or intended to be used to commit the crime. Schemes to commit identity theft or fraud also may involve violations of other statutes, such as credit card fraud, computer fraud, mail fraud, wire fraud, financial institution fraud, or social security fraud. Each of these federal offenses is a felony and carries substantial penalties – in some cases as high as 30-years imprisonment, fines, and criminal forfeiture.

Violations of the Identity Theft and Assumption Deterrence Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service and Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

*There are a number of laws that have been passed at the state and federal level that are designed to reduce identity theft or to provide assistance to victims. At the federal level, Congress enacted the Identity Theft and Assumption Deterrence Act in October 1998 (and codified, in part, at 18 U.S.C. 1028(a)(7)).*

Many state laws and privacy and security-related measures have recently been introduced as identity theft prevention legislation. This also includes laws that limit marketing practices and the use of personal information.

Notice of Security Breach, CA Civil Code 1798.82<sup>1</sup> (formerly Senate Bill 1386) is a sweeping piece of legislation that mandates public disclosure of computer-security breaches in which confidential information of any California resident may have been compromised. It is applicable to every public or private organization and state agency that is conducting business with a resident of California. Under the law, confidential information includes SSNs, California driver's license numbers, account numbers, or credit and debit numbers. This law was passed due to a compromise that occurred at the Teale Data Center in 2002. The Teale Data Center acts as the core IT hosting center for the State of California and thus maintains sensitive information on state employees. Approximately 260,000 state employees had social security and address information compromised as a result of this incident. Companies and organizations that fail to disclose computer security breaches become liable for civil damages or face potential class action lawsuits.

Legislation is not the entire answer to the vexing problem of identity theft. The credit granting and reporting industries must step up their efforts to assist consumers in preventing fraud and in recovering from identity theft. With business environments comprising complex technologies that frequently connect to third-party organizations, it is imperative to perform the appropriate due diligence on any company that is privy to personal information.

## The Challenges Posed by Identity Theft

Examples of commerce complexity occur everyday. As a simplistic analogy, imagine an Olympic torch being passed from one messenger to another to cover a great distance. Each runner demonstrates great care to avoid dropping the torch and to keep the flame from extinguishing while running. Merchants are bearers of individual personal information and the flame is customer trust and, ultimately, profit and success.

Transactions by business-to-consumer and business-to-business companies can involve significant amounts of sensitive and confidential customer data including SSNs, financial account data, credit data, and medical data. A typical transaction can involve several different companies having access to an individual's name, address, credit information, or identifiable information.

*A VISA USA merchant service provider lost their status with VISA due to the egregious nature of a security incident. This incident occurred as a result of the grossly negligent handling of cardholder data and the service provider's non-compliance with VISA USA's Cardholder Information Security Program Standards. As a result, this company is no longer in business.*

To learn more about the VISA USA CISP program, see the case study on page 11.

<sup>1</sup> Other sections of the law include CA Civil Code 1798.29 and 1798.84. Act also referred to as the California Database Protection Act or the California Security Breach Information Act.

Each of these companies, often service providers, would have access to data. In some cases, access to necessary data would be provided. It is common, however, for businesses to provide service providers with more access controls and/or data than is necessary to perform the transaction. For example, a credit card purchase may be seen by a third-party provider that maintains the merchant's service protection plan, a call center that is outsourced to another provider and the billing company that supports the account maintenance. As the personal information moves away from the data source or point of data collection, the care level often diminishes.

This introduces a potential problem for businesses. Some regulated industries (financial services and health care) are required to obtain assurances from affiliates and service providers that they maintain appropriate security and privacy practices. Companies may communicate in their Web privacy statement that the appropriate control levels are applied. This is typically only relevant to that particular company. For businesses that do state their affiliates and third parties, they must employ the appropriate controls. The business challenge is to decide how and through what mechanisms (e.g., audit, contracts and Service Level Agreements [SLA] ) the requirement will be enforced.

In addition to taking due care in handling customer data, the responsibility of the business becomes less clear if and when there is unauthorized access to data. There are so-called "notification laws" that require businesses to notify customers when certain unencrypted customer data is improperly accessed. For example, business customers providing services that grant them access to personal data may or may not be obligated to notify the other companies within the supply chain and/or the offended individual.

Unfortunately, these problems are not unique to merchants processing credit card data. These issues are also prevalent in organizations handling credit reports, health care data, and personal financial information such as banking records and home mortgage information.

## **Solutions to Remedy Identity Theft**

### **FOR THE MERCHANT**

Although subjective, an organization can accurately identify weak links in its supply chain through adopting sound policies. Building and instituting staunch standards and ensuring that these practices are carried out throughout the supply chain will enable an organization to have assurances that there are no weak links.

The best practices and standards to which an organization adheres can be enforced throughout the supply chain. Third-party vendors can be contractually obligated to allow for a systems audit to ensure that they are maintaining the established standards of good practice. Additionally, in the event of a discovered vulnerability in the supply chain, an organization can set guidelines in its contract with third-party vendors to enforce a timeline for remedy. If this timeline is not honored, an organization can penalize the offending third-party vendor. Therefore, through contractual agreements with third-party providers, an organization can effectively prevent the occurrence of weak links in its supply chain.

There are measures organizations can take to protect against the potential damages identity theft poses to the merchant supply chain. Businesses can perform preventative measures to avoid identity theft through identifying or mending weak links in its supply chain. These measures are outlined below:

#### **Preventative Measures to Avoid Identity Theft**

- Develop a strategy similar to one of VeriSign's Business Protection Plans to identify key failure modes, i.e. the compromise of personally identifiable information.
- Choose service providers and supporting services that can maintain the security and privacy of customer data.
- Require attestations from suppliers on adequacy of policies and security and privacy measures.
- Address data privacy, security parameters, and requirements in service agreements and contracts with service providers.
- Develop and enforce privacy and security policies.
- Develop procedures and guidelines to support policies. This includes a comprehensive incident response plan that takes into account failure responses for all points in the merchant supply chain.
- Perform regular scanning assessments to ensure that processing systems are securely configured.
- Perform intrusion detection and monitoring to identify when incidents occur.

#### **Identify Weak Links in the Supply Chain**

- Conduct a privacy and security assessment.
- Assess interfaces with third parties.
- Review access control policies and limitations and require "least know" and "need-to-know."
- Regularly review third-party agreements and activity of service provider.
- Conduct regular vulnerability assessments and contractually obligate third-party companies within the supply chain to do the same.

**Remedy Any Weak Link Where Possible**

- Harden any vulnerabilities.
- Institute 24x7 monitoring similar to the type of program offered through a Managed Security Services Provider.
- Require by contract or SLA that service providers implement measures and maintain customer data security and privacy.
- Limit access to data on a need-to-know only basis.

A responsive organization will view protecting its customers from identity theft as the responsible thing to do as well as a sound long-term business strategy. Toward this end, companies should consider all aspects of identifying and notifying customers when informed of a “scam” involving their name, products or services. When a scam or problem does occur, companies should address the issue internally in a forthright manner with as many identified facts as possible. Companies should also strive to comply with appropriate government regulations.

A complementary strategy is to adopt a corporate-wide consumer privacy policy and implement a secure data-handling regime based on generally accepted fair information practice principles. The five core principles of individual privacy protection for the consumer are as follows:

**Notice/Awareness** – The consumer should be given notice of a business’ information practices prior to the acceptance of personal information.

**Choice/Consent** – The consumer should be given options as to how information collected from them may be used beyond what is necessary to complete the present business transaction.

**Access/Participation** – The consumer should have the ability to access and view data about him or her and contest the accuracy, completeness, and timeliness of the data.

**Integrity/Security** – The consumer should be assured that the business will only use reputable sources for information and cross reference it against multiple sources, offer consumer access to the data, and destroy or convert data to an anonymous form.

**Enforcement/Redress** – The consumer should be assured that the preceding principles would be effective through enforcement and redress.

**FOR THE CONSUMER**

Identity theft victims can spend months or even years using their own money to try and rectify the disaster perpetrators have made of their name and credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing, automobiles or even get arrested for crimes they did not commit. Generally, victims of credit and banking fraud are liable for no more than the first \$50.00 of the loss per 15 USC sec 1643. In many cases, the victim will not be required to pay any part of the loss. However, they are often left with a bad credit report and must spend a significant amount of time regaining their financial health.

In terms of impact, however, the real cost may be the emotional vulnerability most victims experience. Victims often report receiving little help from overworked law enforcement agencies as they attempt to untangle the web of deception that has allowed another person to impersonate them.

The first step in regaining an identity is to contact the fraud departments of any one of the three major credit bureaus to place an alert on the victims credit file. The fraud alert requests creditors to contact the victim before opening any new accounts, or making any changes to their existing accounts. As soon as the credit bureau confirms the victim's fraud alert, the other two credit bureaus will be automatically notified to place fraud alerts, and all three-credit reports will be sent to the victim free of charge.

Additionally, the FTC recommends that identity theft victims take the following steps:

- Close the accounts that have been tampered with or opened fraudulently. Use the ID Theft Affidavit<sup>2</sup> when disputing new unauthorized accounts.
- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of the crime.
- File a complaint with the FTC. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations.
- Consumers can also call 1-877-ID THEFT, the FTC's toll-free ID Theft Hotline, where counselors help consumers who want or need more information about dealing with the consequences of identity theft.

Despite fraud alerts placed on credit reports, the ordeal may be far from over. Accounts may still be opened in the victim's name, providing a continuing nightmare. Regaining identity requires patience, vigilance, and determination.

<sup>2</sup> For more information on the ID Theft Affidavit, visit: <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>

## Conclusion

As companies continue to enlist the Internet to expedite business processes, the incurred security risk grows in accordance. The worldwide adoption of e-commerce has fostered an illicit opportunity for criminals and as a result, any person with a credit card or even a simple bank account is at risk for identity theft.

With potential damages ranging from aiding terrorist efforts to loss of brand to unauthorized money transfers, identity theft has proven to be a serious issue for organizations and consumers alike. Organizations must be diligent in learning and understanding the security challenges presented by the Internet and assume the appropriate responsibility for the information customers entrust them to safeguard. Not giving the issue the attention it requires demonstrates corporate irresponsibility and with increasing federal involvement, repercussions such as consumer lawsuits could lead to financially damaging results to the organization as well. Even organizations that feel they have taken the appropriate precautions must consider any third-party affiliates involved in the transaction process. Securing each link of the merchant supply chain is critical to the ultimate protection of a consumer's personal information. Therefore, organizations must ensure that each third-party affiliate is equally as assiduous in their efforts to safeguard personal customer information.

It is imperative for organizations to assume the lion's share of responsibility for the war against identity theft and take whatever precautions necessary, whether by law or by principal, to protect their customers' personal information. While consumers can address an identity theft incident by following basic complaint filing procedures, it is an ordeal that may take years to fully rectify. An organization, on the other hand, has the opportunity and responsibility to proactively put the appropriate security measures into effect to ensure that thieves cannot access their client's personal information. In the end, protecting customers from identity theft is a sound, long-term business strategy for any organization.

## VISA CASE STUDY

In April 2000, VISA introduced its Cardholder Information Security Program (CISP). Approved in October 1999 and mandated June 2001, the program was created specifically for merchants and service providers who process, store or transmit cardholder data.

CISP defines a standard of due care and enforcement for protecting cardholder information, wherever it is located. Given the high priority the payment industry places on maintaining the confidentiality and integrity of account and personal data, the CISP requirements are directed to all entities that store, process or transmit cardholder information. CISP is built upon 12-basic security requirements along with over 100-detailed sub-requirements.

The 12 CISP requirements are as follows:

- Install and maintain a working firewall to protect data.
- Keep security patches up-to-date.
- Protect stored data.
- Encrypt data sent across public networks.
- Use and regularly update anti-virus software.
- Restrict access by “need-to-know.”
- Assign unique ID to each person with computer access.
- Don’t use vendor-supplied defaults for passwords and security parameters.
- Track all access to data by unique ID.
- Regularly test security systems and processes.
- Implement and maintain an information security policy.
- Restrict physical access to data.

CISP compliance is required of all entities storing, processing or transmitting VISA cardholder data. VISA Members must comply with CISP and are responsible for ensuring the compliance of their merchants and service providers for all payment channels, including retail (brick-and-mortar), mail/telephone-order, and e-commerce.

Separate and distinct from the mandate to comply is the validation of CISP compliance. Validation is a fundamental and critical function that ensures appropriate levels of cardholder information security are maintained. This effort involves ongoing compliance validation of VISA merchants and service providers. VISA has prioritized validation of CISP compliance based on the volume of transactions and the potential risk and exposure introduced into the VISA System by merchants and service providers.

Merchants will verify compliance through their acquirer; service providers will verify compliance directly with VISA.

Compliance with the CISP requirements allows merchants and service providers to protect their information assets and meet the obligations of the VISA payment structure. CISP compliance can also add a level of security to customers who are concerned about the use of their data. For more information about CISP, refer to the Visa Web site at [www.visa.com/cisp](http://www.visa.com/cisp).

## About VeriSign

VeriSign Inc. (NASDAQ:VRSN) delivers critical infrastructure services that make the Internet and telecommunications networks more intelligent, reliable and secure. Every day VeriSign helps thousands of businesses and millions of consumers connect, communicate, and transact with confidence.

For more information on VeriSign's full line of security services, visit:

**[www.verisign.com](http://www.verisign.com).**

**Note:** In February 2004, VeriSign acquired Guardent, a recognized leader<sup>3</sup> in Managed Security Services. Guardent's security consulting and managed services are integrated into VeriSign's solution portfolio.

<sup>3</sup> See <http://www.gartner.com/reprints/guardent/118599.html> for more information.