



WHITE PAPER

The Merchant Supply Chain

Dangers, Challenges, and Solutions



Where it all comes together.™



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	8
+ Conclusion	9
+ Visa Case Study	10



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 nonquantifiable 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 during the past 12 months, 3.23 million consumers, or 15 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. The two main types of identity theft are account takeover and true-name fraud. Account takeover occurs when a thief acquires existing credit information for an account holder and purchases products or services masked as that person. True-name fraud, or application fraud, happens when the thief uses data such as a Social Security number (SSN) and other identifying information to create new accounts in another person's name. Victims of true-name fraud are often unaware of the crime because the thief will have used a different billing address. By 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 with which one person can assume the identity of another for fraudulent and nefarious purposes presents the real danger of this issue. 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 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 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 strategies like hacking.

The danger to consumers is that identity theft can result in loss of credit, the inability to rent or own a home, criminal charges, or difficulty gaining employment. Identity thieves may make unauthorized purchases of big-ticket items for quick resale, open wireless or phone-service accounts, obtain auto loans, sign up for new credit card accounts, or file for bankruptcy to avoid debts or eviction. A person can also use a stolen identity when he or she is arrested, leaving the victim with the possibility of outstanding warrants. In short, identity theft can wreak havoc on a consumer's life in both immediate and long-term ways. Since the theft may go unnoticed by the consumer for some time, and because some thieves continue to engage in fraudulent activity, the crime may not be resolved for years.

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

When an identity thief targets a consumer for criminal activity in order to make unauthorized purchases, the victim is placed at financial risk. However, when a consumer is targeted for identity theft to carry out terrorist activity, the act poses a threat to the general public. At a U.S. Senate hearing held September 9, 2003, for example, 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 the terrorist attacks of 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 U.S. government earn one of its first terrorism convictions.

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

Identity theft has an impact on businesses as well through loss of credibility, brand identity, 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 involves Acxiom, one of the world's largest specialists in customer and information management. The company was forced to admit that it 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 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 schemes involve sending a mass email, supposedly originating from a business, that claims a problem exists with a consumer's account or that the customer needs to cancel a mistakenly placed order. The message provides a link that will take the consumer to a Web site, with a plausible-sounding URL, that resembles the actual company's valid site. The consumer will then be asked to input personal information such as credit card or bank-account numbers, or personal-identification numbers or SSNs. The information is then gleaned for identity theft.

Another scam gaining ground is the theft of data found on employment sites. The media has reported on stories of résumé rip-offs, in which a vast number of employment histories 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 a company has an older version of his or her résumé and is asked to update and provide new information such as a SSN.

The Identity Theft and Assumption Deterrence 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."

A Visa USA merchant-services provider lost its 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 noncompliance with Visa USA's Cardholder Information Security Program (CISP) 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 10.

Under the act, “means of identification” refers to a name or a SSN, as well as a credit card number, an electronic serial number for a cellular telephone, 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, plus a fine and 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 those regarding 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 much as 30 years in prison, fines, and criminal forfeiture.

Violations of the act are investigated by federal law-enforcement agencies, including the U.S. Secret Service, the U.S. Federal Bureau of Investigation, the U.S. Postal Inspection Service, and the U.S. Social Security Administration's Office of the Inspector General, and federal identity-theft cases are prosecuted by the U.S. Department of Justice.

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

The Notice of Security Breach Act (California Civil Code 1798.82¹; formerly California 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 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 security compromise that occurred in 2002 at the Teale Data Center, which acts as the core IT hosting center for the State of California government and thus maintains sensitive information on state employees; Social Security and address information for about 260,000 of these workers was compromised as a result of this incident. Companies that fail to disclose computer-security breaches become liable for civil damages or potentially face class-action lawsuits.

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

¹Other sections of the law include California Civil Code 1798.29 and 1798.84. The act is also referred to as the California Database Protection Act or the California Security Breach Information Act.

The Challenges Posed by Identity Theft

Examples of commerce complexity occur every day. As a simplistic analogy, imagine an Olympic torch being passed from one relay runner to another to cover a great distance. In turn, each person demonstrates great care to avoid dropping the torch and to keep the flame from becoming extinguished. Merchants, likewise, 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 and financial-account, credit, and medical data. A typical transaction can involve several companies having access to an individual's name, address, credit information, and other identifiable data.

It is common, however, for businesses to provide service providers with more access controls and/or data than is necessary to perform a 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 outsourced to another provider, and the billing company that supports account maintenance. And, as the personal information moves away from the data source or point of data collection, the care level often diminishes.

This factor introduces a potential problem for businesses. Some regulated industries, such as 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 online privacy statement that appropriate control levels are applied. This claim, however, is typically relevant only 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—audit, contracts, and service-level agreements (SLAs)—the requirement will be enforced.

In addition to taking due care in handling customer data, the business' responsibility becomes less clear if and when unauthorized access to data occurs. So-called notification laws require businesses to inform 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. They are also prevalent in enterprises 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 any enterprise is by nature subjective about its operations, it can accurately identify weak links in its supply chain by adopting sound policies. Building and instituting staunch standards and ensuring that these practices are carried out throughout the supply chain will enable a company to be assured that no weak links exist.

The best practices and standards to which an enterprise 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, a company can set guidelines in its contract with third-party vendors to enforce a timeline for remedy. If this schedule is not honored, the company can penalize the offending third-party vendor. Therefore, through contractual agreements with third-party providers, the business can effectively prevent occurrences of weak links in its supply chain.

Enterprises can take measures to protect against the potential damages identity theft poses to the merchant supply chain. Businesses can perform the preventative measures outlined below to avoid such theft by identifying or mending weak links in its supply chain

Preventative Measures to Avoid Identity Theft

- Develop a strategy similar to one of the VeriSign® Business Protection Service to identify key failure modes (such as 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, including 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” status for access to sensitive information.
- Regularly review third-party agreements and activity of service provider.

The best response to identity theft is to protect yourself from it in the first place. One critical component is to share credit card numbers and other confidential information only with Web sites you trust—and only with ones that use SSL to encrypt these transmissions. Look for the VeriSign Secured™ Seal to identify sites able to protect your confidential information from spying eyes, and enjoy added safety while you do business online.



- 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 24/7 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.

A responsive enterprise 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 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 principles of fair information practice. The five core principles of individual privacy protection for consumers include:

Notice/awareness—Consumers should be given notice of a business' information practices prior to acceptance of personal information.

Choice/consent—Consumers 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—Consumers should be able to access and view data about themselves and contest its accuracy, completeness, and timeliness.

Integrity/security—Consumers should be assured that the business will use only reputable sources for information and cross reference it against multiple sources, offer consumers access to the data, and destroy data or convert it to an anonymous form.

Enforcement/redress—Consumers 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 to rectify the disaster perpetrators have made of their name and their credit record. In the meantime, victims may lose job opportunities, be refused loans, education, housing, and automobiles, or even get arrested for crimes they did not commit. Generally, according to 15 USC sec. 1643, victims of credit and banking fraud are liable for no more than the first \$50 of the loss. In many cases, however, victims are not required to pay at all. 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: they 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 uncompromised identity is to contact the fraud departments of any one of the three major credit bureaus to place an alert on the victim's credit file. The fraud alert asks 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 credit reports from all three credit bureaus will be sent to the victim free of charge. In addition, the FTC recommends that identity-theft victims take the following steps:

- Close the accounts that have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit² when disputing new, unauthorized accounts.
- File a police report and obtain a copy to submit to creditors and other entities that may require proof of the crime.
- File a complaint with the FTC, which maintains a database of identity-theft cases law-enforcement agencies use for investigations.
- Call 1-877-438-4338, the FTC's toll-free ID Theft Hotline, where counselors provide information about dealing with the consequences of identity theft.

Even after fraud alerts are placed on credit reports, however, the ordeal may be far from over for the victim. Accounts may still be opened in the victim's name, and regaining one's identity requires patience, vigilance, and determination.

Conclusion

As companies continue to enlist the Internet to expedite business processes, security risks grow 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.

Potential damages range from unauthorized money transfers to loss of brand to aiding terrorist efforts, and 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 use of the Internet presents and must assume appropriate responsibility for the information customers entrust them to safeguard. Organizations demonstrate corporate irresponsibility when they do not give the issue the attention it requires, and, as a result of increasing federal involvement, repercussions such as consumer lawsuits could lead to financially damaging results for organizations as well.

Even businesses that believe they have taken the appropriate precautions must consider any third-party affiliates involved in transactions. Securing each link of the merchant supply chain is critical to the ultimate protection of a consumer's personal information. Therefore, enterprises must ensure that each third-party affiliate is equally diligent in its efforts to safeguard 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 principle, to protect customer data. Although consumers can address an identity-theft incident by following basic complaint-filing procedures, it is an ordeal that may take years

²For more information on the FTC's ID Theft Affidavit, visit www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf.

to fully rectify. An organization, on the other hand, has the opportunity and responsibility to proactively put appropriate security measures into effect to ensure that thieves cannot access customer data. In the end, protecting customers from identity theft is a sound, long-term business strategy for any company.

Visa® Case Study

In April 2000, Visa introduced its Cardholder Information Security Program (CISP). Approved in October 1999 and mandated in 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 on 12 basic security requirements and more than a hundred detailed subrequirements.

The 12 CISP requirements include:

- 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 antivirus software.
- Restrict access by need-to-know status.
- Assign a unique identity for each person with computer access.
- Don't use vendor-supplied defaults for passwords and security parameters.
- Track all access to data by unique identification.
- 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 online and offline retail businesses and mail-order or telephone-order companies.

Separate and distinct from the mandate to comply is the validation of CISP compliance. Validation is a fundamental and critical function that ensures that 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 verify compliance through their acquirer; service providers 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 concerned about the use of their data. For more information about CISP, refer to the Visa Web site at www.visa.com/cisp.

+ Learn More

For more information about VeriSign Managed Security Services and Global Security Consulting, please call 650-426-5310 or email enterprise_security@verisign.com.

Visit us at www.Verisign.com for more information.