MASTERCARD INTERNATIONAL SECURITY AND RISK MANAGEMENT: CREDIT CARD FRAUD

Michael Cornish ■ Kathleen Delpha ■ Mary Erslon

Executive Summary

Credit card fraud is a growing concern of global proportions. Resourceful criminals are finding creative ways to capture private credit card holder account and identification information, and are using this information for fraudulent acquisitions of everything from personal care items to cars to home loans. Because of the universal reach of the Internet, criminals are easily able to perpetrate their crimes from anywhere in the world.

The costs of credit card fraud reach nearly U.S. $2.5 billion annually. Internet fraud alone accounts for nearly 3% of Internet sales, or 30 times higher than credit card fraud rates in the "physical world." While consumers are generally held harmless for credit card fraud, the payment industry and merchants absorb the losses from fraudulent purchases, and its participants continually search for ways to detect and prevent them.

MasterCard International, the licensor and franchisor of the MasterCard branded family of payment products, is appropriately concerned about credit card fraud, since MasterCard research shows that the majority of their cardholders are alarmed about credit card fraud and the risk to their personal and financial information. MasterCard and other credit card systems are susceptible to two general categories of threats for fraudulent activities: Internal threats and external threats. Internal threats are those that evolve from collusion within the credit card system itself. However, internal threats are often mitigated by following good employment practices such as conducting employee background checks, and implementing strong controls that prevent unauthorized access to sensitive information and tracking authorized access. External threats come from forces outside the credit card system. External threats are very difficult for the credit card system to mitigate because there are so many points of compromise outside of their control.

In particular, two methods of credit card fraud, the "card-not-present" and identity theft methods, are increasing in incidence. A review of the literature and focused conversations with MasterCard employees revealed that credit card fraud is underreported in general and that the exact amount of losses due to fraudulent activities on cards is unknown. Merchants who accept MasterCard branded products are burdened with the expenses associated with fraudulent purchases, but consumers are left with a real burden when they fall victim to identity theft. Consumer and merchant concerns about using and accepting credit cards have led MasterCard to intensify their security and risk management activities. A review of security and credit card research and reports, and personal interviews with MasterCard International security executives, comprises the basis for our study of MasterCard's security measures targeted at combating card-not-present and identity theft credit card fraud.

Payment card security management comprises the collective set of activities to develop and implement physical card designs that combat fraud. Risk management comprises the activities that protect the system's participants from credit and fraud risk. In this paper, we review MasterCard's security and risk management activities, and offer case studies of specific measures that MasterCard has taken to combat these growing threats. With the urging of consumers, merchants and payment companies, the growing fraud problem has also caught the attention of state and federal legislators. We will provide an overview of key legislation introduced and/or passed to combat credit card fraud and identity theft.

The payment industry is working diligently to provide Information Technology (IT)-enabled solutions for early detection and capture of fraudulent credit card transactions. MasterCard employs the following applications and services to manage fraud: Address Verification System, Combined Warning Bulletin, Common Points of Compromise, Fraud Velocity Monitor, Issuers Clearinghouse Service, MasterCard Alerts, MasterCard Internet

Gateway Services, MasterCard SecureCode, Merchant Alerts to Control High Risk, Merchant Online Status Tracking, NameProtect Partnership, RiskFinder, Site Data Protection, and System to Avoid Fraud Effectively. At best, such solutions may prevent many fraudulent transactions, saving dollars and distress for consumers, merchants, and the payment industry in general. Unfortunately, because of the Internet, numerous fraudulent credit card transactions take place abroad, where perpetrators are not subject to United States laws or penalties. The best the credit card industry can hope to achieve is to quickly detect when a new type of threat emerges, then devise electronic and procedural countermeasures to mitigate the threat.

Fighting credit card fraud is not solely the responsibility of the credit card systems, however. General guidelines for all participants in credit card transactions emerge as "best practices": for consumers, merchants, credit card issuers and acquirers, and the payment systems themselves. "Best practices" may be as simple and low-technology as a consumer keeping track of receipts for credit card transactions, or as complex and high-technology as implementing software-enabled neural networks designed to detect data anomalies that are predictors of fraudulent activity. In general, all participants in the credit card transaction process must be conscientious about protecting private identification and financial information, monitoring credit card activity, and keeping aware of fraud trends in the credit card world.

A TYPICAL VICTIM OF CREDIT CARD FRAUD

Jane D. looked worriedly at the charges for a new stereo system on her latest MasterCard statement. Jane had not purchased a stereo system, and she had many questions: Who had access to her credit card number? Where was the stereo system? Was she liable for the charges?

Jane D., like nearly 25 million other adults each year[1], is a victim of fraud. With over 600 million MasterCard credit cards in circulation[2], it is not surprising that incidence of credit card fraud is a major concern for all participants in the payment industry. Credit card fraud costs merchants more than U.S. $2 billion a year[3]. The cost of fraud is passed on to the consumer in the form of higher prices, interest rates and fees.

Fraudulent credit card activities present unique challenges for MasterCard and other credit card companies, financial institutions that issue and process credit card transactions, and the consumer. The credit card industry is working hard to enhance fraud prevention and detection techniques. This paper will review the methodology of credit card transactions, explore case studies of card-not-present transactions and identity theft credit card transactions, present Information Technology (IT)-enabled solutions to these fraudulent transactions, discuss legislative efforts to combat credit card fraud, and offer "best practices" for prevention and detection of credit card fraud for consumers, merchants, and card processors.

[1] www.ftc.gov/opa/2004/08/fraudsurvey.htm, viewed October 17, 2004.
[2] "MasterCard Corporate Fact Sheet." www.mastercardinternational.com/docs/corporate_fact_sheet_0804.pdf, viewed October 18, 2004.
[3] Bhatla, Jej Paul, Prbhu, Vikram, and Dua, Amit, "Understanding Credit Card Frauds" *Card Business Review # 2003-01*, June 2003, 1-15.
[3] "MasterCard Corporate Fact Sheet," www.mastercardinternational.com/docs/corporate_fact_sheet_0804.pdf, viewed October 18, 2004.
[5] MasterCard International SEC Form 8K – February 3, 2004, www.sec.gov/Archives/edgar/data/1141391/000095012304001154/y93767e8vk.txt, viewed October 18, 2004, 3.

MASTERCARD LICENSES AND FRANCHISES THE MASTERCARD BRAND TO ITS MEMBER BANKS[4]

MasterCard International, Inc. is a private stock membership association owned by its 25,000 member banks. MasterCard International is the licensor and franchisor of the MasterCard branded family of payment products; the individual member banks are the franchisees. The family includes credit card and debit card products which are targeted at both businesses and consumers. The MasterCard payment brand is number two by spending volume globally, behind Visa, and is accepted at more than 22-million merchants and over 900,000 Automated Teller Machines (ATMs) worldwide. MasterCard cardholders transacted 13.2-billion times for a gross value of U.S. $1.27 trillion in calendar year 2003. [5]

As franchisor, MasterCard International sets and maintains brand standards and operating rules, and provides commonly needed IT services like transaction processing, settlement, and risk management. Combined, these standards, rules, and services enable seamless payment brand acceptance and global interoperability. MasterCard's goal for people like Jane D. is for her to have universal acceptance of her credit card and to have the same quality experience, wherever she is on the globe.

A common misconception about MasterCard is that it issues credit cards, sets annual and other fees, determines annual percentage rates (APRs), and solicits merchants to accept cards. All of these activities are outside of MasterCard's scope. MasterCard's member banks are responsible for all activities revolving around issuance of cards and signing merchants to accept them.

MasterCard International is a multinational corporation, with global headquarters located in Purchase, New York, USA. Its technology headquarters, known internally as Global Technology and Operations (GTO), are located in O'Fallon, Missouri, USA. MasterCard employs about 4,000 people globally, about 2,000 of which work for GTO.

MasterCard's CIO is the head of GTO, and reports directly to the President and CEO. In addition to classic IT functions like data center operations, network operations, architecture management, and systems development, the CIO is responsible for member services, security and risk management, and technology business management.[6]

CREDIT CARD TRANSACTIONS "GO WITH THE FLOW" OF INFORMATION

For you to understand the complexities of managing credit card fraud, it is critical to understand how the credit card business is structured. The credit card business operates under the notion of an acceptance brand, like MasterCard's interlocking red and yellow circles. The acceptance brand is essential for matching up the two elemental participants: Merchants and Cardholders.

The merchant is a business or governmental entity which accepts credit cards as a form of payment for goods or services it provides. A merchant displays signage for one or more acceptance brands prominently on its store front, counter tops, marketing literature, and website to announce that it accepts like-branded cards for payment.

The cardholder is a person who has been issued a credit card bearing a brand mark, for use to purchase goods and services at participating merchants. A cardholder may be an individual consumer or business person. The cardholder is trained to look for brand signage to recognize merchant outlets that accept the credit card.

Many other participants enable cardholders and merchants to exchange value using branded credit cards as a payment device. Participants vary significantly depending on the structure of the credit card system. There are two basic structures in the credit card industry: the open system and the closed system.

The Open Payment System: Two or More Participants Cooperate to Process Payment for Mutual Benefit

An open payment system is typified by two or more cooperative entities that collectively issue credit cards and facilitate acceptance at merchants, for mutual benefit. The open system model is also referred to as the *Interchange Model*, in recognition of its interactive and reciprocal nature. The cooperative participants are often referred to collectively as associations or

[6] Fisher, Bill. Pers. Comm. VP Processing Strategy, MasterCard International. Interviewed by telephone by Mike Cornish, October 26, 2004.

networks. The associations and networks define extensive rules to govern how transactions and value flow between the participants, and they may be regional, national, or global in scope. Using the U.S. as an example, a regional network may operate within a small number of contiguous states, whereas a national association would operate within all 50 states. The U.S. market had dozens of regional networks at one time, such as *NYCE*, *HONOR*, *PULSE*, and *BankMate*. Over time, most of the regional networks were bought up and consolidated into a few national networks. Prominent national networks in the U.S. are *STAR* and *Interlink*. There are two players at the global level: MasterCard and Visa.

Figure 1 depicts the business relationships and flows of information between participants in MasterCard's open system.

Besides the Merchants and Cardholders, the participants in an open system typically perform one or more of the following roles. The numbers in parentheses correspond to the circled number on the figure.

Acquirer: A financial institution which sponsors merchants into the open payment system (1). The institution accepts merchant deposits for credit card transactions, and reimburses the merchants for the value of the transactions, less any fees. Acquirers are financially liable for the actions of their merchants, so they take great care in screening merchants to make sure they are legitimate.

Issuer: A financial institution which issues credit cards to businesses and consumers, for use in paying for goods and services (2). The institution determines credit worthiness, assigns credit lines, sets interest rates and fees, prints and mails statements, and collects payments. Each Issuer reimburses Acquirers for purchases made by its cardholders, and then collects future payments plus fees and interest from the cardholders. Issuers are financially liable for the actions of their cardholders, so they carefully screen applicants to ensure they only issue cards to those who represent acceptable risks.

Processors: Usually third parties, who provide merchant and/or card issuing processing services on behalf of acquirers (3) and issuers (4). Some very large

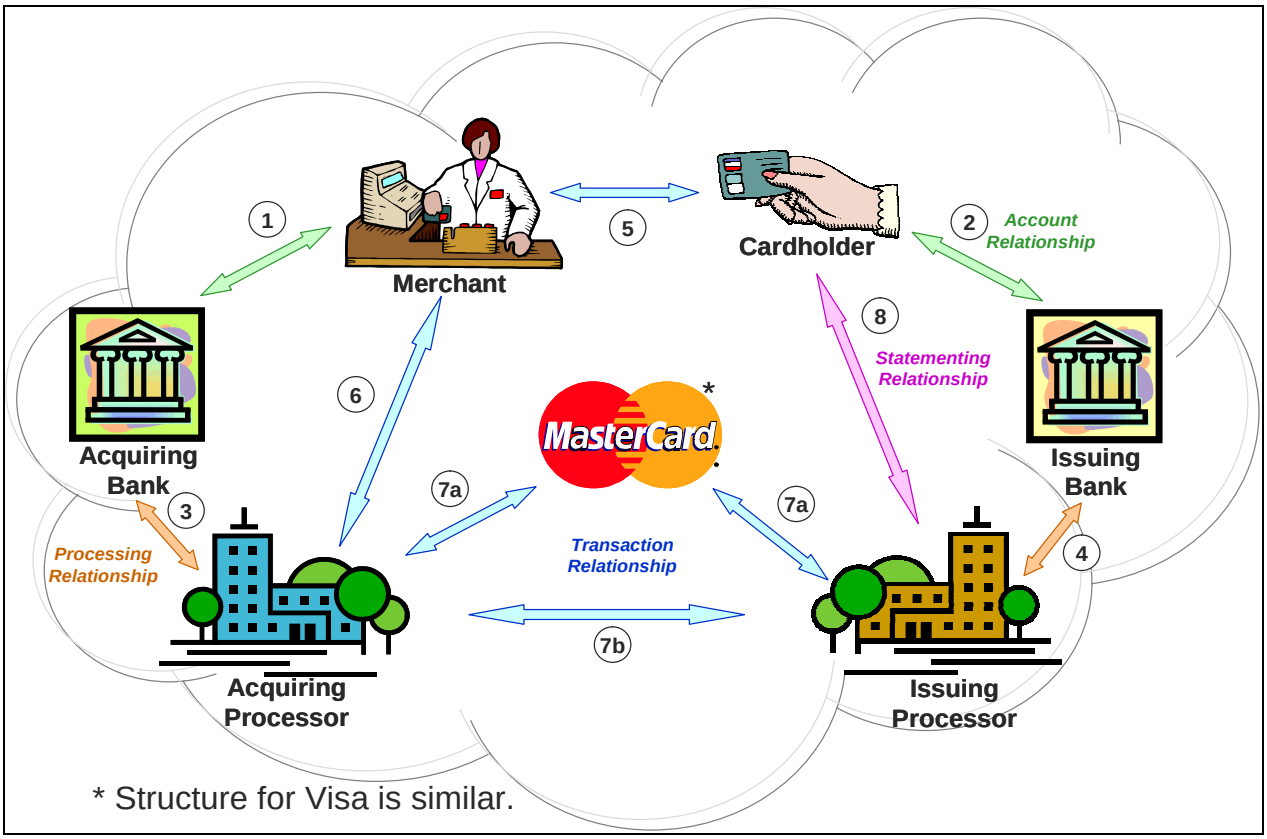


Figure 1: Open System - Interchange Model

and very small member institutions do process their own business in-house, but they are more the exception than the rule. Third-party processors range in breadth and scope from performing simple services like Point-of-Sale terminal management and customer service call center operation, to providing full-service, turn-key operations for merchants (6) and issuing processing (8).

Association or Network: A cooperative group of financial institutions, each of whom behave in the role(s) of acquirer and/or issuer, to enable use of credit cards for value exchange between participating merchants and cardholders (5). The association or network often provides an underlying technology infrastructure and business applications to facilitate transaction processing and payments between participants (6), (7a). Note: Some Acquirers are also Issuers, and so it sometimes happens that a transaction occurs involving a card issued and a merchant sponsored by the same member bank. This situation is called an "on-us" transaction. In such cases, the transaction would likely be processed in-house without being sent to the association. A similar case occurs when a given pair of Acquirers and Issuers shares the same processor. Transactions between the pair of members would likely be processed internally within the processor's network (7b).

Figure 2 depicts the standard transaction and financial flows necessary to complete a typical MasterCard credit card cardholder purchase at a merchant acceptance outlet. The processing steps are as follows:

1) The Merchant initiates a request for authorization from its point-of-sale (POS) terminal or electronic cash register (ECR). The request flows to the acquiring processor, through MasterCard's network to the issuing processor.

2) The issuing processor makes a credit decision, and returns a response indicating an approved or declined transaction back to the merchant device, following the reverse path of the request.

3) Assuming the authorization request was approved, the merchant and cardholder complete the sale. The merchant submits the completed sale at the end of its business day, in a batch of all transactions completed during the day.

4) The Acquiring bank makes a deposit into the merchant's bank account to reimburse the merchant for the accumulated value of the deposited batch of transactions, less any pre-

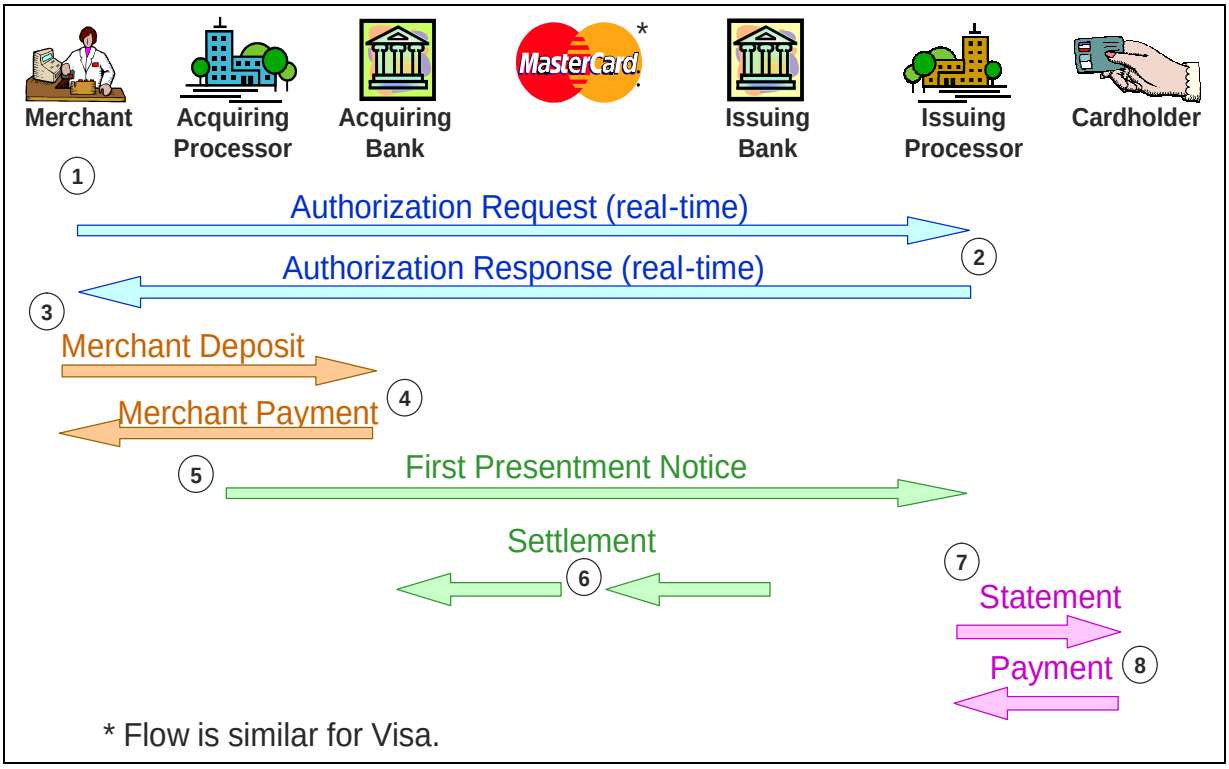


Figure 2: Open System - Interchange Transaction Flow

agreed discounts and fees.

5) The acquiring processor submits the transaction as a first presentment into MasterCard's clearing process. The transaction is grouped in a file with all of the daily transactions for all of the merchants processed by the acquiring processor. MasterCard's clearing process collects, sorts, and redistributes all of the transactions to each appropriate issuing processor. The issuing processors post the transactions to the appropriate cardholders' accounts.

6) The association collects funds from issuers and distributes them to acquirers, for the net value of all cleared transactions.

7) The issuing processor produces monthly statements and sends them to cardholders.

8) Cardholders make payments against their credit card accounts.

The Closed Payment System Makes Its Own Rules

A closed payment system is typified by a single entity that both issues credit cards and facilitates acceptance at merchants. The entity defines its own rules to govern how transactions and value flow between itself and its merchants. Examples of closed systems vary in scope from house brands, to national and global brands. Home Depot is an example of a house branded credit card. Home Depot cardholders may only use their credit cards in Home Depot and Expo stores. Discover card is an example of a national brand, and American Express (AMEX) is an example of an international brand.

Figure 3 depicts the business relationships and flows of information between participants in American Express' closed system.

Unlike an open system, there are no separate Acquirers and Issuers in American Express' closed system. Merchants contract directly with American Express for card acceptance (1), and American Express issues cards directly to all of its cardholders (2). American Express performs all of the Acquirer and Issuer functions described for the open system above. American Express also provides the underlying technology infrastructure and business applications to facilitate transaction processing for merchant acceptance (3), (4a). Due to high levels of consolidation of merchant processing across the payments industry, American Express handles transactions from Acquiring Processors as well (4b).

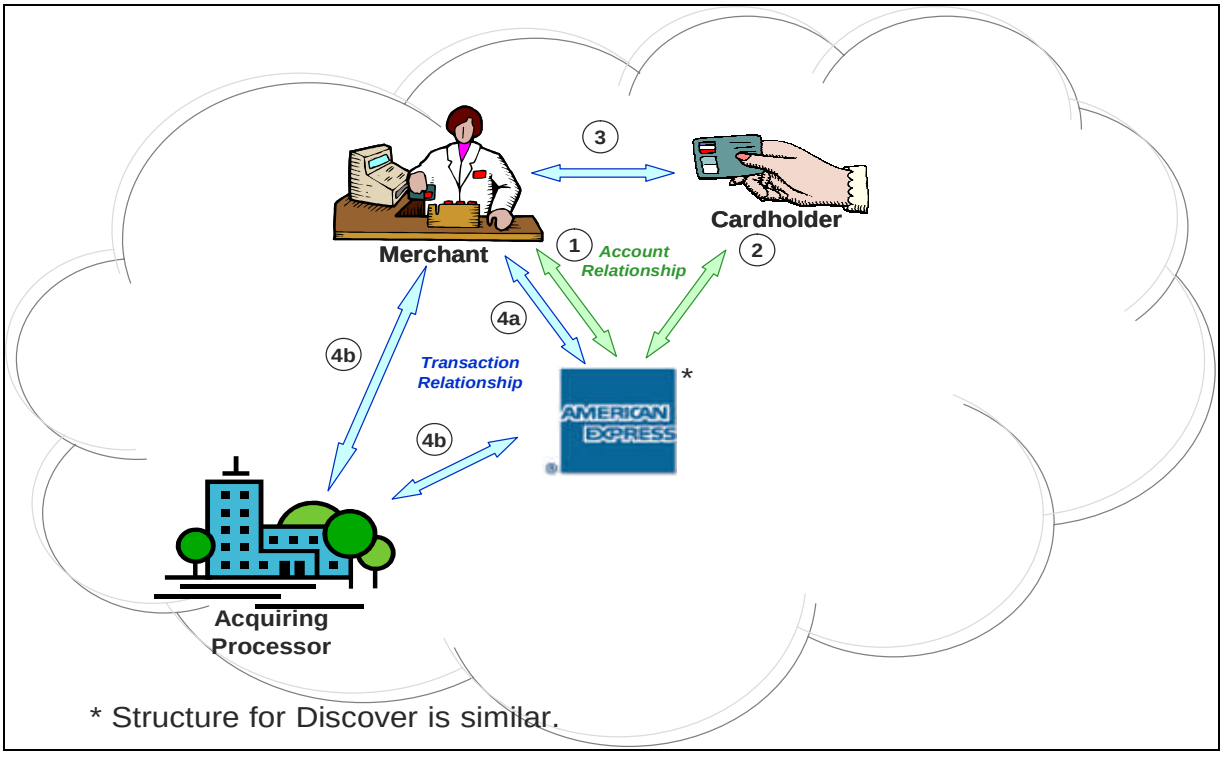


Figure 3: Closed System

Figure 4 depicts the standard transaction and financial flows necessary to complete a typical AMEX credit card cardholder purchase at a merchant acceptance outlet. The processing steps are as follows:

1) The Merchant initiates a request for authorization from its point-of-sale (POS) terminal or electronic cash register (ECR). The request flows to AMEX either directly through AMEX's network, or through an Acquiring Processor.

2) AMEX makes a credit decision, and returns a response indicating an approved or declined transaction back to the merchant.

3) Assuming the authorization request was approved, the merchant and cardholder complete the sale. The merchant submits the completed sale at the end of its business day, in a batch of all transactions completed during the day.

4) AMEX makes a deposit into the merchant's bank account to reimburse the merchant for the accumulated value of the deposited batch of transactions, less any pre-agreed discounts and fees.

5) AMEX posts the transactions to the cardholders' accounts.

6) AMEX produces monthly statements and sends them to cardholders.

7) Cardholders make payments against their credit card accounts.

Open and Closed Credit Card Systems are Subject to Two Classes of Threats

Open and closed credit card systems are susceptible to two general categories of threats for fraudulent activities: internal threats and external threats. While the most serious threat might be an attack that diverts some or all of the billions of dollars flowing through the credit card systems daily, the most prevalent attacks are those that expose individual account and private consumer identifying information. Of the two, private consumer identifying information is the most lucrative. Account information, e.g., account numbers and expiration dates, allows thieves to make fraudulent purchases; private consumer identifying information, e.g., names, addresses, and Social Security numbers, allows thieves to obtain fraudulent credit.

Internal threats: "An Inside Job"

Internal threats are those that evolve from collusion within the credit card system itself. These threats may appear at any point along the distribution channel where employees have access to account or consumer information, and vary in severity in relation to the quantity and quality of information accessible. Note that open credit card systems likely have more exposure to internal threats by virtue of the sheer number of

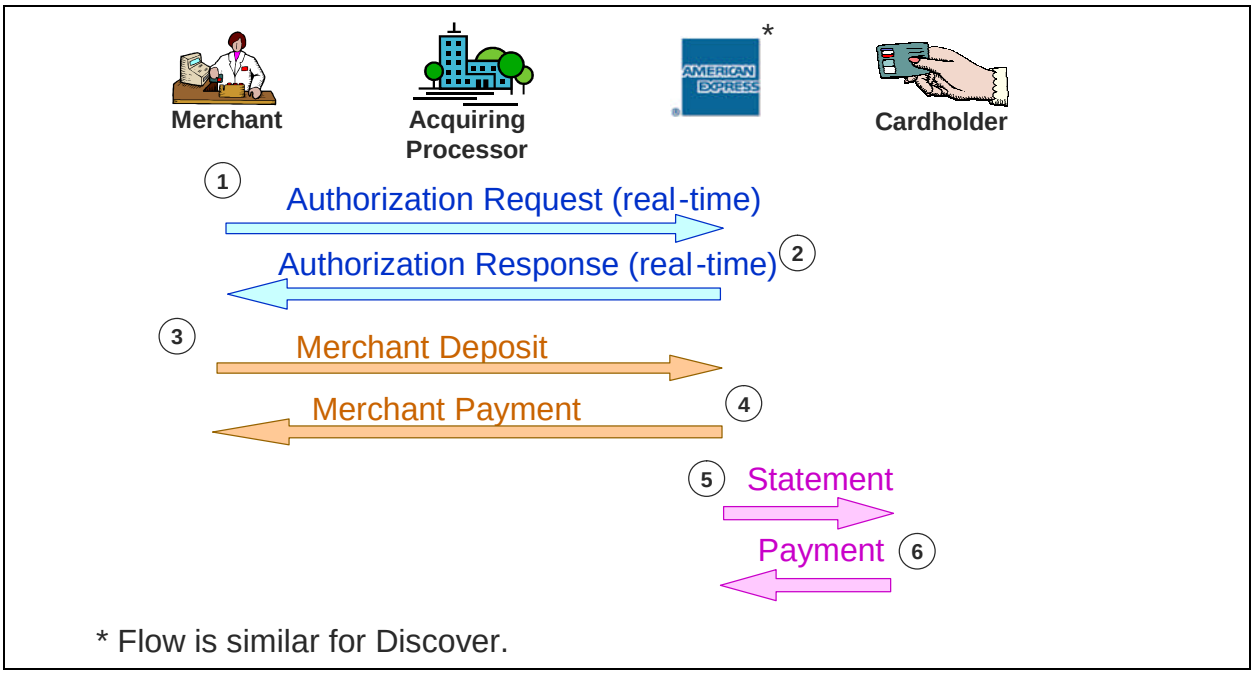


Figure 4: Closed System - Typical Transaction Flow

participants in the system. Examples of internal threats are:

- A merchant or acquiring processor employee who conspires to collect good account numbers and expiration dates.
- An issuer or issuing processor employee who collects private customer identifying information such as Social Security numbers, names, and addresses

Internal threats are often mitigated by following good employment practices such as conducting employee background checks, and implementing strong controls that prevent unauthorized access to sensitive information, and tracking authorized access. Additional mitigation techniques are defined in the section on Best Practices found later in this report.

External Threats: "Let Me Make You an Offer You Can't Refuse"

External threats come from forces outside the credit card system. While the threats may originate from the isolated actions of a few individuals, they are more often the result of highly organized criminal enterprises. The criminal organizations form networks or syndicates of sources of account and identifying data, and use the ill-gotten information to perpetrate large-scale fraud enterprises. A source could be anyone who has compromised a place where account numbers or private consumer identification information is stored. Sources can run the gamut from private citizens, to public servants, to sophisticated computer hackers.

Office workers can be a lucrative source of information. Many businesses hold account numbers and private identification information on file. Social Security Numbers are collected by many businesses and public entities alike, including insurance companies, health care providers, schools, and government agencies. Crime syndicates approach people who work in such offices and use extortion or promises of financial reward to gain cooperation in collecting the valuable information.

Seemingly every day there is a news story about another database that hackers compromised to expose credit card account numbers or Social Security numbers (see Figure 5). While early hackers were motivated by the thrill of breaking into a bank's database, current-day hackers are motivated by the financial gains they may realize by selling information to the crime syndicates.

External threats are very difficult for the credit card systems to mitigate because there are so many points of compromise beyond their control. The best the credit card systems can hope to accomplish is to quickly detect when a new type of threat emerges, then devise electronic and procedural countermeasures to mitigate the threat. In the end, the threat emergence-mitigation cycle continues in a positive feedback loop, in a cold war-like escalation between the criminal organizations and the credit card systems. The criminals hatch a new scheme and successfully run it for awhile. Eventually the credit card systems catch on, and develop effective

Figure 5: Hackers in the News

countermeasures. In a Darwinesque example of survival of the fittest, a few criminals are caught and crime organizations are taken down, but the rest adapt and find new ways to compromise the systems.

Under Attack: Credit Card Fraud Results from Threats Executed Against the System

Credit card fraud is defined as "when an individual uses another individual's credit card for personal reasons while the owner of the card and the card issuer are not aware of the fact that the card is being used.[7]"

Credit card fraud can take many forms, but generally result from threats carried out against the credit card system. The most common type of credit card fraud stems from lost or stolen cards or card numbers, which can lead to the thief using the card or card number for criminal purposes over the telephone or the Internet (card-not-present purchases). Identity theft occurs when a thief uses another individual's identifying facts to perpetrate an economic fraud[8], such as taking over a financial account (i.e. a credit card account), or applying for credit. Counterfeit cards can be created by copying a legitimate cardholder's data onto a generic card. Legitimate card numbers can be obtained by "*skimming*," which copies data from a card's magnetic stripe into an electronic device; *account number generation*, or software programs that generate valid credit card numbers and expiration dates; and *hacking*, where an individual gains unauthorized access to an individual or corporate computer system for the purpose of stealing data[9]. Overall, credit card counterfeiting is decreasing however, largely because of industry measures such as the addition of holograms and the Card Verification Value (CVV), a three-to-four digit number that is printed (not embossed) on the back or front of all US-issued credit cards[10]. A newer type of credit card fraud, called "*phishing*," occurs when a victim is solicited via e-mail to visit a sham website of a "trusted institution" to "confirm or renew" private account information. In the phishing scam[11], this account information is then used to place fraudulent credit card orders over the Internet, or to perpetrate identity fraud by making financial applications in the cardholder's name. Figure 6 depicts the incidence of fraud by method, as documented by Bhatla, et al in their recent study on credit card fraud[12]

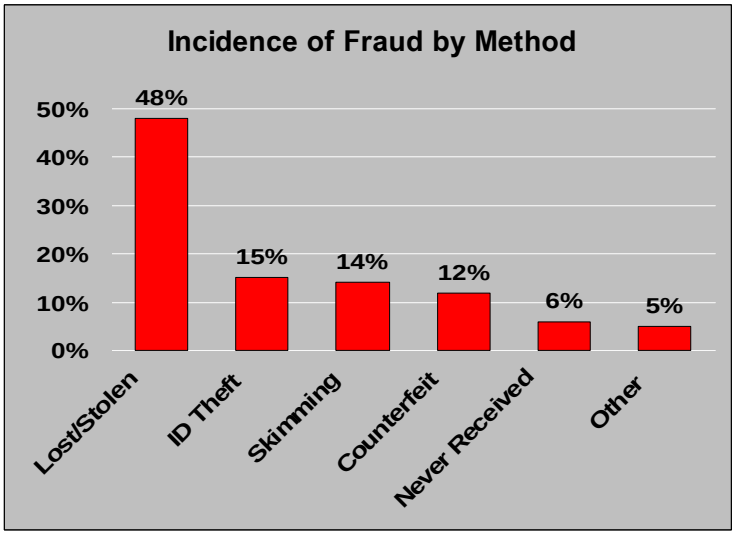


Figure 6: Incidence of Fraud by Method. Bhatla[14]

Our Top Story Tonight: Credit Card Fraud Reaches Nearly U.S. $2.5 Billion Annually!

A review of the literature and focused conversations with MasterCard employees[13] revealed that credit card fraud is underreported in general and that the exact amount of losses due to fraudulent activities on cards is

[7] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds"1.

[8] Saunders, Kurt M., and Zucker, Bruce, "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption of Deterrence Act" *International Review of Law, Computers & Technology*, August 1999, 183-192.

[9] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds," . 4-6.

[10] Anonymous, "Bank Card Report: Counterfeiting Falls, But Other Fraud Remains," *ABA Banking Journal*, Vol. 78, No. 9,. 60.

[11] "New Leahy Bill Targets Internet "Phishing" That Steals $2 b./yr. From Consumers," July 2004. www.leahy.senate.gov/press/200404/070904c.html, viewed October 20, 2004.

[12] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds," 2.

[13] Fisher, Bill. Pers. Comm. VP Processing Strategy, MasterCard International. Interviewed by telephone by Mike Cornish, October 26, 2004

unknown[14]. However, credit industry analyst reports estimate that fraudulent card activity in 2002 is between U.S. $2 and U.S. $2.5 billion[15],[16]. The rate of Internet fraud ranges between 2% and 3% of sales[17],[18], and is estimated at 30 times higher than credit card fraud rates in the "physical world."[19]

SHELTER FROM THE STORM: SECURITY AND RISK MANAGEMENT

Payment card *security management* comprises the collective set of activities to develop and implement physical card designs that combat fraud, and to design policies and procedures to protect and control stocks of blank cards to prevent them from being stolen and turned into counterfeit cards. *Risk management* comprises the activities that protect the system's participants from credit and fraud risk. Credit risk is the potential for financial losses resulting from making poor credit decisions when member banks issue credit cards or sign up merchants for acceptance. Fraud risk is the potential for financial losses resulting from fraudulent activities. Many of the everyday activities of the credit card systems are targeted at managing risk. The practice of requiring merchants to request authorization for purchases mitigates both credit and fraud risk. Issuers practices of pulling credit histories before issuing new credit cards also mitigates credit risk. The scope of this paper is limited to managing fraud risk.

MasterCard: "Protecting Brand Integrity and Managing Fraud Risk"

MasterCard's Security and Risk Management group is wholly contained in the GTO organization, and reports to the CIO. The group's mission is to "Protect brand integrity and manage fraud risk through best in class core and value added services with integrated end to end solutions to help position MasterCard as the Global Payments Leader.[20]"

The group is responsible both for conducting investigative field work, and for analyzing fraud trends and developing mitigation strategies.

The field work team is largely comprised of retired law enforcement officers who entered the private sector. The officers typically came from detective squads, the Secret Service, and the Federal Bureau of Investigation, where they investigated white collar financial crimes and organized crime. Their principle duties are to work with fraud officers from the member banks and to cooperate with local, national, and international law enforcement agencies to investigate and crack major cases of fraudulent credit card use.

The fraud analysis team is a combination of credit card fraud experts and systems analysts. The team collects fraud reporting data from MasterCard's member institutions and analyzes it to discern emerging changes in fraud patterns. When a given type of fraud makes a significant directional change, they research and investigate with member banks to determine the underlying reasons. Often the change results from some new attack. Based on their findings, the team works with industry security specialists, fraud officers at the member institutions, and sometimes even scientists, to further study the problem and devise counter-measures.

The Security and Risk Management group is the business owner for most of the services and applications targeted at fraud management. Each of the services and applications is targeted to address one of the following fraud management goals:

Goal	Description
Awareness	Identify and communicate positive/negative changes in fraud trends
Detection	Detect when specific fraud is likely to have occurred
Prevention	Prevent fraudulent transactions

The following are brief descriptions of the services and applications that MasterCard employs to manage

[14] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds," 2.
[15] Ibid.
[16] www.epaynews.com/statistics/fraud.html, viewed October 22, 2004.
[17] www.merchant911.org/fraud-trends.html, viewed October 22, 2004.
[18] www.epaynews.com/statistics/fraud.html, viewed October 23, 2004.
[19] www.retailindustry.about.com/cs/lp_Internet/a/gl_cs111803.htm, viewed October 21, 2004.

[20] "Security & Risk Mission & Overview." Document, MasterCard International, February 24, 2003.

fraud.[21] Note those denoted by an asterisk (*) have business owners outside of Security and Risk Management, but are still important pieces of the overall risk management strategy:

Address Verification System*: Permits merchants who accept Card Not Present transactions to verify that the cardholder billing address provided by the person making the purchase matches the address on the issuer's database.

Combined Warning Bulletin: Maintains a database of credit card account numbers that are blocked from use. The accounts are restricted because they were reported as lost, stolen, counterfeit, or otherwise compromised. Any authorization request for a restricted account automatically receives a "pick up card" response.

Common Points of Compromise: Analyzes merchant use histories for account numbers reported in fraud, to identify any common merchants at which the accounts were used prior to the frauds occurring. A high incidence of accounts for a common merchant indicates a probability that the merchant has a collusive employee who is stealing account numbers.

Fraud Velocity Monitor: Analyzes velocity (numbers of uses and accumulated spending) by account, and flags accounts with patterns of rapid growth in activity. Flagged accounts are reported to issuers for their further investigation.

Issuers Clearinghouse Service: Screens credit applications against a database of recent applications to detect unusual patterns in increased credit applications. Key applicant data are matched against information like names, addresses, Social Security numbers, and phone numbers. Known fraudulent and non-existent addresses are also checked.

MasterCard Alerts: Distributes high-priority information about new fraud schemes and alerts about specific accounts and merchants to member institutions.

MasterCard Internet Gateway Services*: Provides a payment gateway which eCommerce merchants may integrate into their catalog shop-and-buy websites, to facilitate credit card payments without actually handling credit card account details.

MasterCard SecureCode: Defines a set of rules and underlying technology that permits a cardholder to define a "password" that must be successfully entered on a participating website, before a sale can be completed.

Merchant Alerts to Control High Risk: Identifies merchants who have accumulated fraudulent activity that exceeds MasterCard's rules for percentage of fraudulent transactions to total sales.

Merchant Online Status Tracking: Tracks merchants that MasterCard has terminated from the system because of excessive fraudulent activity. Screens merchant registrations against the database of terminated merchants to keep bad merchants out of the system. Key registration data are matched against information like owner's name, address, Social Security number, employer id number, and Dunn & Bradstreet number.

NameProtect Partnership: A contracted service that monitors the worldwide web, searching for websites which are promoting and exchanging information for purposes of credit card and identity theft fraud.

RiskFinder: Screens approved authorization transactions against a neural network designed to detect data anomalies that are predictors of fraudulent activity, and produces a score that indicates the likelihood of fraud. An alert message is sent to the card issuer for any transaction for which the fraud score exceeds the issuer's pre-established threshold.

Site Data Protection: A service provided to evaluate a merchant's website against best practices for eCommerce security, and to make recommendations which the merchant should consider to strengthen its site against attacks.

System to Avoid Fraud Effectively: Collects and summarizes member reported fraudulent transaction information, to aid the Security and Risk Management team and the member institutions in tracking fraud trends.

Figure 7 depicts how each of the above applications or services addresses the Security and Risk Management group's fraud management goals, for the various types of fraud.

[21] "Application Portfolio: Security & Risk Applications." Internal document: Word document. MasterCard International, March 27, 2003.

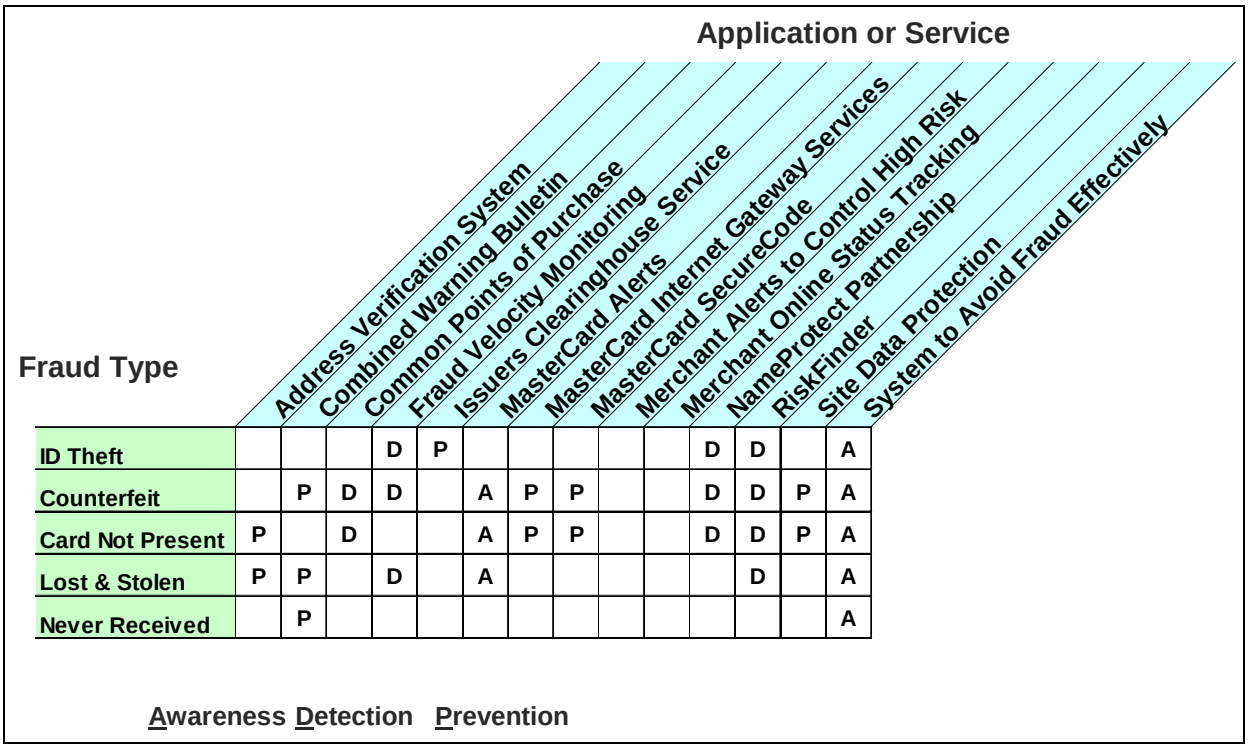


Figure 7: Fraud Types Addressed by Application or Service.

"I WASN'T EVEN THERE": CARD-NOT-PRESENT FRAUD

Card-Not-Present: No Way to Dispute that a Purchase Wasn't Made

Card-not-present credit card fraud poses a great threat to merchants, because they are not protected with the physical verification features present in "brick and mortar" businesses. Because neither the card nor the cardholder are present at the point of sale, the merchant is unable to verify the signature or photo identification of the cardholder[22], so there is no way to dispute a cardholder claim that a purchase was not made. In these situations, the merchant assumes the full risk of credit purchases.

Online and telephone shoppers expect fast decisions for purchases. Because of the explosion of eCommerce, card-not-present transactions are a necessity. Merchants, credit card processors and credit card companies are asking the credit card systems for real-time tools and support for online credit decisions,[23] and the systems are working to provide a variety of multi-level IT-enabled solutions.

Understandably, Credit Card Holders are Concerned about Credit Card Fraud

Electronic transactions are estimated to have a worldwide market potential of U.S. $3 trillion-plus. Still, MasterCard research shows that 90% of online buyers worry that their personal and financial information may be at risk, and 71% are concerned about credit card fraud.[24] How valid are their fears?

It is very difficult to determine the actual incidence and prevalence of credit card fraud, and there are several reasons why. First, many cardholders do not report fraud to law enforcement agencies – they simply contact their issuing bank, and the fraudulent charge is

[21] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds," 1.

[23] Anonymous. "Credit Risk Analysis Makes e-Commerce Safer" *ABA Banking Journal*. Nov 1999, Vol. 91, Iss. 11; 54.

[24] "MasterCard SecureCode for Online Merchants." Online security document for merchants at www.mastercardmerchant.com/docs/securecode/Mercahnt_Brochure.pdf, viewed October 20, 2004.

credited.[25] Similarly, merchants may simply absorb the fraudulent charges, and not think it necessary to report the fraud to law enforcement agencies.[26] Lastly, credit card companies such as MasterCard and Visa don't release the credit card fraud information they do have. Linda Locke of MasterCard, as quoted in an article published on msnbc.com, said in response to figures released by a security agency about credit card fraud: "We don't release that kind of data…that seems way overstated…we will not validate that number…we think that number is incredibly overstated."[26]

MasterCard reports that card-not-present fraud incidents account for between 80 and 84% of credit card fraud.[27] Other sources report that online fraud rates are up to thirty times higher than those in the physical world, representing a revenue loss of about U.S. $1.6 billion, or about 2% of all online sales in 2003.[28] Projected losses to Internet merchants in 2005 are expected to be between U.S. $5 and U.S. $15 billion.[29]

The Merchant Risk Council is a non-profit organization of merchants, vendors, financial institutions and law enforcement agencies. Its members "share the common goal of protecting and encouraging the thriving online commerce industry by establishing best practices for cybersecurity," as well as work with law enforcement agencies to catch and prosecute cyber criminals. A 2003 Merchant Risk Council survey of eCommerce fraud shows two key trends:[30] 1) Merchants are spending more on fraud prevention - 17% of merchants spent more than 2% of their revenue on fraud prevention in 2003; and 2) Chargeback rates are down – only about 10% of online businesses have chargeback rates greater than 1%, and the number of online merchants with chargeback rates of less than 0.35% is increasing proportionately.

"Now, Where Did I Put My Credit Card?" Causes and Contributing Factors to Card-Not-Present Fraud

Lost or Stolen

Credit cards or credit card numbers can be stolen by very conventional, "low technology" means such as a thief sorting through trash to retrieve discarded cards, credit card receipts, or credit card statements, which is known as "dumpster diving." Some credit cards are simply "lost" by the cardholder; left behind at a point of sale. Credit cards may also be removed from purses or briefcases at work, school, or other settings if left unattended by the cardholder. Several legislative rulings, to be discussed later in this paper, limit the information printed on credit card receipts and statements in an effort to combat this type of fraud.[31] Consumer best practices presented later in this paper may also help to combat low technology theft of credit cards or card numbers.

High Tech, Low Touch

Valid credit card numbers may also be obtained for card-not-present schemes by significantly more "high technology" means. This includes phishing as well as online "auctions" or false merchant sites designed to lure purchasers into believing they are making legitimate purchases at valid retail web sites. Other schemes, such as account number generation, may be beyond a cardholder's control. Credit card companies, issuers and processors are developing IT-enabled solutions to combat the high technology schemes at multiple levels. Two such IT-enabled solutions licensed by MasterCard will be discussed as case studies.

---

[25] www.merchant911.org/fraud-trends.html, viewed October 22, 2004.
[25] Ibid.
[26] Sullivan, Bob, "Credit Card Leaks Continue at Furious Pace" http://msnbc.msn.com/id/6030057/. Viewed October 22, 2004.
[27] Bennett, RA. "I Didn't Do It" *US Banker*, Vol. 111, No. 12, December 2001, 48.
[28] "Online Fraudsters Take $1.6B Out of 2003 eCommerce." *CyberSource*, www.retailindustry.about.com/cs/lp_Internet/a/bl/cs111803.htm, viewed October 20, 2004.
[29] Bhatla, Jej, Prbhu, and Dua, "Understanding Credit Card Frauds," 2.
[30] Merchant Risk Council Press Release, www.merchantriskcouncil.org/press.php?p_press_id+13, Feb 3, 2003, viewed October 21, 2004

[31] Micci-Barreca, D. "Unawed by Fraud." *Security Management*, Vol. 47, No. 9, September 2003,75.

En Guard: MasterCard's Efforts to Combat Card-Not-Present Fraud Security

SecureCode: Cardholder Authentication

MasterCard SecureCode for Online Merchants is a "global e-commerce solution enabling cardholders to authenticate themselves to their issuer through the use of a unique, personal code."[32] (Visa has a licensed counterpart called "Verified by Visa," or VbyV.) SecureCode requires a merchant "plug-in," or software module, to be deployed on the merchant's web site. It also requires the merchant to use a data transport mechanism and purchase compatible processing support from their transaction processor. Though the software module and accessories represent a cost to the merchant, the merchant gets explicit evidence of an authorized purchase from the cardholder's issuer, and gets the security and protection of fully guaranteed online payments and protection from chargebacks.[33,34,35] Though it is a relatively new security platform, MasterCard believes it will be effective and endorsed a mandate for MasterCard issuers to implement support for SecureCode effective November 1, 2004.[36]

Case Study: eTronics has eFraud Problems.[37] eTronics is a top ten Internet consumer electronics retailer that has over 200,000 customers and processes more than 300,000 orders annually. Their annual sales exceed U.S. $65 million. In 2002, eTronics had credit card chargeback costs of more than U.S. $1 million for the year. eTronics first implemented a multi-level anti-fraud process, but it was costly and cumbersome. In 2003, they implemented SecureCode. eTronics says it is "too soon to tell" the impact of SecureCode on their return on investment, but they are "optimistic and enthusiastic" – and anxious for all card issues to be required to support SecureCode.

Case Study: Gone Phishing with Citibank. Mike Cornish received the e-mail message in Figure 8 in his home e-mail account, stating that his request for an "Express Transfer" had been received. He is, in fact, a Citibank client. Compare the two web sites and observe the similarities between the false "phishing" web site (Figure 9) and the true website for MyCiti.com (Figure 10). The phishing site looks remarkably authentic. Cornish called Citibank customer services and the representative confirmed that the email was bogus. She said she had recently handled many similar calls from other customers.

"I Know Who You Are and I Saw What You Did": Neural Networks Modeling Technologies Profile Cardholder Spending Patterns

MasterCard RiskFinder™ is a neural network system developed by MasterCard and Fair Isaac. It is a modeling technology that builds detailed profiles of each individual cardholder's spending patterns and behavior, which are updated with every transaction.[38] RiskFinder enables transactions to be "scored" based on the profiles of cardholder patterns and behavior, existing patterns of fraud, and merchant trend data. If a transaction scores above the established "transaction score threshold," the issuer will contact the cardholder to be sure no fraudulent activity has occurred. By leveraging this processing network to identify purchases which exceed threshold scoring, it is hoped that fraudulent activities will be identified.[39] As of 2004, it has saved issuers up to 50% in fraud losses.[40]

---

[32] "MasterCard SecureCode for Online Merchants." Online security document for merchants at www.mastercardmerchant.com/docs/securecode/Merchnt_Brochure.pdf, viewed October 20, 2004.

[33] Ibid.

[34] White Paper: Security Best Practices: Protecting Your Business. www.authorizenet.com/files/securitybestpractices.pdf. Viewed November 10, 2004.

[35] "Credit Card Authentication." Paymentech Solutions. www.paymentech.net/sol_frapro_carnotpre_crecaraut_page.jsp. Viewed November 10, 2004.

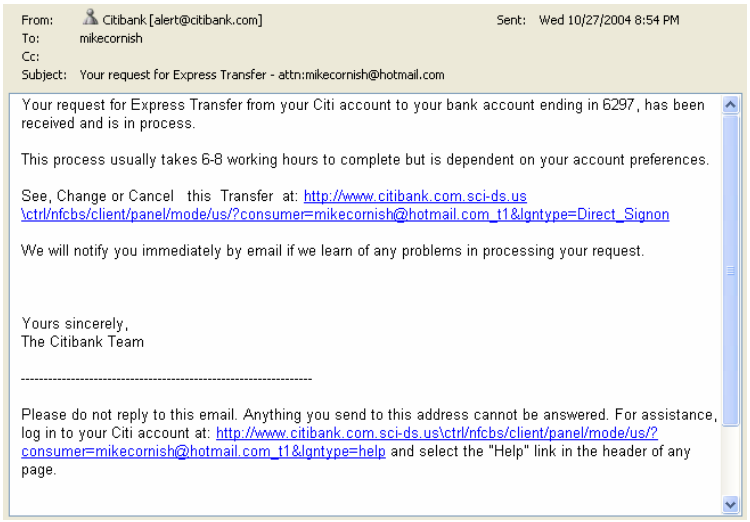
[36] "MasterCard SecureCode Case Study: eTronics." 2003. www.mastercardmerchant.com/docs/SC_Case_Study-eTronics.pdf. Viewed October 21, 2004.

[37] Ibid.

[38] MasterCard RiskFinder. "Solutions." www.fairisaac.com/cgi-bin/MsmGo.exe?grab_id=13&page_id=655872&query=RiskFinder&hiword=RiskFinder+, viewed October 21, 2004.

[39] "MasterCard and NYCE Enter Into Agreement." 2004. www.tgc.com/dsstar/00/0718/101932.html, viewed October 21, 2004.

[40] MasterCard RiskFinder. "Solutions." www.fairisaac.com/cgi-bin/MsmGo.exe?grab_id=13&page_id=655872&query=RiskFinder&hiword=RiskFinder+, viewed October 21, 2004.



From: Citibank [alert@citibank.com] Sent: Wed 10/27/2004 8:54 PM
To: mikecornish
Cc:
Subject: Your request for Express Transfer - attn:mikecornish@hotmail.com

Your request for Express Transfer from your Citi account to your bank account ending in 6297, has been received and is in process.

This process usually takes 6-8 working hours to complete but is dependent on your account preferences.

See, Change or Cancel this Transfer at: http://www.citibank.com.sci-ds.us \ctrl/nfcbs/client/panel/mode/us/?consumer=mikecornish@hotmail.com_t1&lgntype=Direct_Signon

We will notify you immediately by email if we learn of any problems in processing your request.

Yours sincerely,
The Citibank Team

Please do not reply to this email. Anything you send to this address cannot be answered. For assistance, log in to your Citi account at: http://www.citibank.com.sci-ds.us\ctrl/nfcbs/client/panel/mode/us/?consumer=mikecornish@hotmail.com_t1&lgntype=help and select the "Help" link in the header of any page.

Figure 8: E-mail to Mike Cornish verifying request for "Express Transfer" to Citi account.

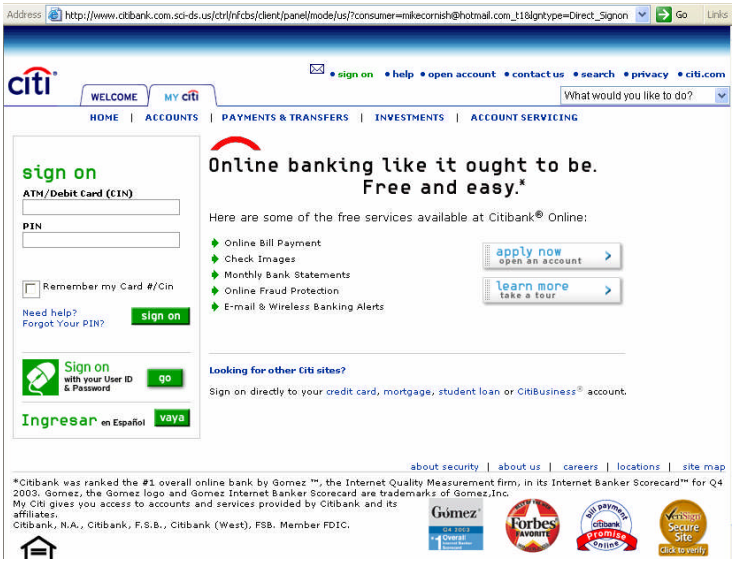


Figure 9: "Phishing" web site for MyCiti.com. Note request for ATM card number and PIN, as well as trademark and official logo.

Figure 10: Authentic web site for MyCiti.com. Note they request User ID and Password, not account number.

Case Study: Venice the eMenace. In the summer of 2003, Kathleen Delpha's 20-year old daughter went to Europe to study art history. Delpha gave her daughter her credit card, and notified the card issuer that her daughter would be taking it to England, southern France, and Florence. Three weeks into the trip, Delpha received a call from the card issuer stating that suspicious charges had posted to her credit card, and the issuer "flagged" the account as irregular. The charges were for two train tickets to Germany, and for an Austrian corporation doing business as a trailer park in Venice. Delpha knew her daughter had no plans to go to Germany, and that her daughter was "not a trailer park kind of girl." The credit card was placed on hold. When Delpha reached her daughter, she learned that, in fact, the charges were legitimate: her daughter had charged train tickets to Germany for a friend in exchange for much-needed cash, and her visit to Venice to see a major art show was expensive, but the trailer park was an inexpensive place to stay. While the charges were legitimate, the neural network worked to identify credit charges that were beyond the threshold established by Delpha's usual purchasing behaviors and those identified as acceptable for her daughter.

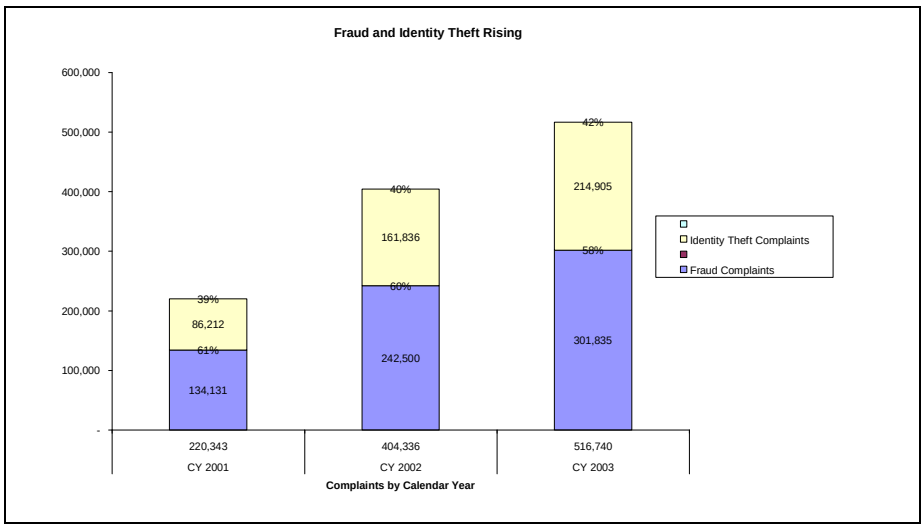


Figure 11: Annual Identity Theft and Fraud Complaints to FTC

IDENTIFY THEFT FRAUD: "Is He Really Who He Says He Is?"

Exactly What is Identity Theft Fraud Anyway?

Law Professor Kurt Saunders has described identity theft as, "the neoteric crime of the information technology era."[41] His definition of identity theft emphasizes the illicit use of another's identifying facts to commit a fraud. The fraud can be anything from obtaining a credit card by using someone else's name, address, and Social Security number on the application for credit, to opening bank accounts, obtaining loans, or signing leases for cars or apartments in the victim's name.[42] Simply put, identity theft is taking on the identity of the victim for malevolent purposes.

I'm Careful, Why Should I Worry About Identity Theft?

The significance of the emergence of this technology-enabled crime is that it has quickly become the number one source of consumer complaints to the Federal Trade Commission,[43] with credit card fraud as the most common form of identity theft annually since 2002.[44] Increasingly, "the weapon of choice is the Internet."[45] Since the FTC began tracking identity theft in 1998, there is clear evidence that fraud and identity theft, "are already much bigger issues than conventional wisdom estimates."[46] David Myron prepared the following chart from FTC data for American Demographics.[47]

The data in Figure 11 illustrates that both forms of complaints are growing each year, and that identity theft is growing at a slightly faster rate than fraud. Whereas identity theft accounted for 39% of complaints registered in 2001, it accounted for 42% by 2003,

[41] Saundersand Zucker, "Counteracting Identity Fraud in the information Age: The Identity Theft and Assumption of Deterrence Act", 184.
[42] Ibid.
[43] Groves, Shanna, "Protecting Your Identity" *Information Management Journal*, May/June 2002, 27-31.
[44] Ibid., 28.
[45] Myron, David, "Stolen Names, Big Numbers" *American Demographics*, September 2004, 36-38.
[46] Ibid., 37.
[47] Ibid.

stealing "nearly U.S. $50 billion in ill-gotten gains in the U.S. last year alone."[48]

This is of concern to more than just the individuals who have their identities stolen. Online sales increase every year, and with the steady growth of fraud and identity theft, it is certain to increase the cost of doing business. Staying ahead of the criminals is the concern of those businesses most likely to be affected.

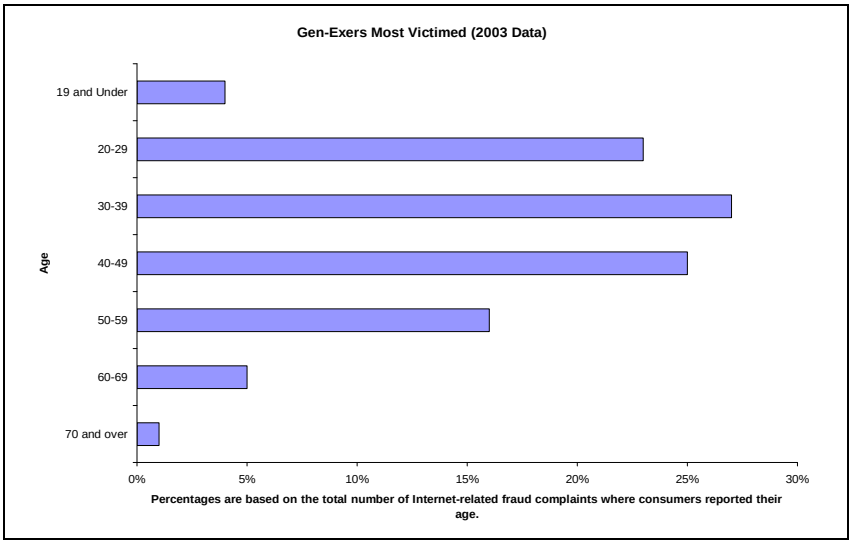


Figure 12: FTC data showing Gen-Xers are most victimized for identity theft.

Another finding of interest by Myron is that Gen-Xers, as compared to other age groups, are most victimized by Internet-related fraud complaints. The chart depicted in Figure 12 is an adaptation of David Myron's analysis of the FTC data.[49]

This is of small comfort for those of us who are not of that generation since it suggests two things. First, since Gen-Xers are more frequent Internet users than their parents; those of us in other generations who regularly shop online are likely at higher risk than others in our own generation. The other thing suggested by this data is that, without intervention, the problem will continue to grow as young, computer-literate children come of age.

Some sources dispute the figures published by the FTC that have led to identity theft being "dubbed 'the fastest growing crime in America'."[50] An industry roundtable jointly organized by the Federal Reserve Board and Gartner, Inc. in February 2004 met to try to achieve a consensus definition of identity theft. The American Bankers Association Senior Federal Counsel, Nessa Feddis, claims that "identity theft is being exaggerated because all kinds of fraud are being redefined as such. 'People call identity theft what they would before have called a stolen check,' says Feddis."[51] Dennis Behrman, an analyst with Financial Insights, an IDC subsidiary, says, "'Identity theft requires sensitive, personal information,' such as someone's Social Security number, in effect a unique, lifelong identifier; 'it can't just be a credit card number being hacked'."[52] Increasingly, financial industry sources are making a distinction between "account takeover/identity theft" and the more common phenomenon of "identity fraud."

Identity fraud is being used to describe situations "where elements of a real person's identity—typically their Social Security number—are blended with made-up elements, such as a false name, to open new accounts."[53] Behrman notes the importance of this distinction is that in the identity fraud scenario, "'the victim is the institution'. The individual's credit history is not tarnished, so they will never know. Meanwhile, when the short-lived account is depleted, 'the bank will register it as a credit loss, not a fraud loss'."[54]

It will be interesting to see how this discussion continues to develop in the coming months and what the consensus will be regarding the definition of identity theft. Those who are critical do not dispute that identity theft is a huge and growing problem. While they disagree with the number of victims, critics like Behrman acknowledge that identity theft will continue to grow in the years ahead.

For the purpose of this paper, we are continuing to use the FTC definition which includes the misuse of an existing credit card account as one form of identity theft.

[48] Ibid.
[49] Ibid., 38.
[50] O'Sullivan, Orla, "ID Theft Overstated? Some Think So" *ABA Banking Journal*, February 2004, 8-10.
[51] Ibid., 8.
[52] Ibid., 10.
[53] Ibid.
[54] Ibid.

Armed Forces	Landlords
Banks	Lawyers
Brokerage Firms	Life Insurance Companies
City or County Commissioners of Revenue	Loan Companies
Colleges	Mutual Funds
Continuing Professional Education Providers	Occupational and Professional Bureaus
Credit Bureaus	Libraries
Credit Card Companies	Realtors
Department of Motor Vehicles	Retail Stores
Doctors, Dentists, Hospitals, Labs	Retirement Plans
Employers, Former Employers	School Systems
Finance Companies	Social Security Administration
Grocery Stores (check cashing clubs)	State Commissioners of Revenue
Health Clubs	U.S. State Department (passports)
Health Insurers	Utility Companies
Internal Revenue Service	Voter Registrars
Investment Service Providers[56]	

What are the Causes and Contributing Factors to Identity Theft Fraud?

When the infamous bank robber, Willie Sutton, was asked the question, "Willie, why do you rob banks?" he answered, "Because that's where the money is." Perhaps more people would adopt Sutton's outlook if there were not federal laws with steep penalties for robbing a bank. Conversely, the under-prosecution of crimes that facilitate identity theft is a contributing factor to its ubiquity. Identity theft is continuing to grow at an alarming rate according to Bruce Townsend, special agent in charge of Financial Crimes Division with the Secret Service, because, "Compared to equally profitable crimes involving drug or gun trafficking, the sentencing for identity fraud is much lighter—and those folks are tough to catch."[55] The methods used to obtain another person's identifying information are varied, but they can be summed up as falling into the following categories that can be described as either low-tech or high-tech, or due to human vulnerability.

[55] Bielski, Lauren, "Identity Theft" *ABA Banking Journal*, January 2001, 27-30.

Low Technology: One Person's Trash is Another Person's Treasure

Similar to methods used to obtain data for card-not-present fraud transactions, low technology methods for identity theft may stem from a lack of personal responsibility (such as improperly disposing of receipts) as well as from information that was purloined from paper records not in the cardholder's control. Identifiers including name, address, birth date, and Social Security number can be found in many computer and paper files of institutions listed in Table 1.

While banks and credit card companies such as MasterCard have multiple levels of security to guard against identity theft, not all of the above institutions are as informed and diligent when it comes to safeguarding personal information.

High Technology: Those Who Can't Hack It Go Phishing

Two major high technology causes that contribute to credit card identity theft are phishing and hacking.

[56] Riordan, Diane A., and Riordan, Michael P., "Who Has Your Numbers?" Strategic Finance, April 2003, 22-26.

Phishing, e.g., "Stealing corporations' identities as a mean to impersonating individuals," [57] has already been discussed in the Card-not-present Case Study. In the context of identity theft however, the greater the number of pieces of personal information obtained by a fraudster, the greater the chance of full-blown identity theft. The Anti-Phishing Working Group estimates that 5% of consumers will respond to requests to visit phony web-sites and enter their account numbers and passwords. More will be said in the upcoming section on the "Payment Industry Efforts to Combat Identity Theft" about actions that corporations are taking to protect the integrity of their websites and copyrighted logos.

A newer phishing scam, "currently spreading online works without your ever having to click on a hyperlink; all that's required to activate the scam is for you to open an infected email." [58] This phishing attack uses the same approach that virus writers take. The phishing scam has been labeled JS/QHosts21-A by an antivirus vendor, Sophos. "The scam involves a Trojan horse that combines with an ActiveX vulnerability in Windows to install itself on your machine invisibly, without warning."[59] The Trojan horse makes changes to your Hosts file, which will later take you to the fraudster's website when you type in the name of a bank website. "They infect you with a Trojan, wait for you to visit a banking site, and then a keylogger grabs your password."[60] This scam is currently only targeting banks in Brazil, and furthermore, up-to-date antivirus software should be able to catch it. But security experts are concerned. Because this approach does not require the creation of a bogus website, there is less work for the hackers, and less chance of there being clues to lead to them. It also exposes the poor security in place at the websites of many banks and financial institutions. "'If your bank is using a static user name and password, that's like leaving the key to your house under your doormat,' says Jochem Binst, director of communications for Vasco data security. 'Using static passwords online is just not secure enough anymore.'"[61]

The technical discussion about this latest form of phishing leads right into the other high-tech method for obtaining information that can be used to perpetrate identity theft: hacking. Hacking can happen on home computers, on merchant sites, and anywhere else where personal information is stored, especially when servers aren't set up correctly. One of the methods used to compromise these computers is a method called end-mapping, which "pings" servers systematically until it finds an open port to exploit.[62]

A massive number of records were compromised in an August 2004 incident through an intrusion on a computer at the University of California, Berkeley. The computer contained information for a research project involving the personal information of 1.4 million recipients and providers of In Home Supportive Services from the California Department of Social Services. Berkeley IT staff, through the use of intrusion detection software, determined that the database was compromised by hackers. A report in Network World Fusion indicated that, "the malicious hacker exploited a vulnerability in 'commercially available database software' and compromised the computer, but they don't know if the attack was targeted, speculating that malicious hackers possibly discovered the system by scanning for machines running vulnerable versions of the database software."[63]

Human Vulnerability: The Mission-Critical IT Handlers

Human vulnerability remains as one of the most compelling threats to security. Stakeholders should be cautioned against a false sense of security that can be created through the use of technology security systems. James Bauerle writes that "technology system designers, contractors, administrators, or any others who come in contact with the technology all occupy a position at the center of the hourglass of enterprise information management that affords them unparalleled ability to damage the enterprise if they are so inclined. They should be screened no less rigorously than executive officers trusted to lead the organization."[64]

Bauerle goes on to warn that when a destructive force is directed from within the institution that even a thorough set of security policies and procedures, diligently enforced and regularly updated, combined with up-to-date security technology forming a platform for protecting the integrity of the institution and its records, will not be a sufficient defense. He counsels that "it is

[57] O'Sullivan, Orla, "Gone Phishing" *ABA Banking Journal*, November 2003, 7-8.
[58] http://msn.pcworld.com/news/article/0,aid,118489,00.asp viewed, November 19, 2004.
[59] Ibid.
[60] Ibid.
[61] Ibid.
[62] Bielski, Lauren, "Striving to Create a Safe Haven Online" *ABA Banking Journal*, May 2003, 53-59.
[63] http://www.nwfusion.com/news/2004/1020califdisc.html, viewed October 25, 2004.
[64] Bauerle, James F., "Golden Eye Redux," *The Banking Law Journal*, March 2003, p. 11.

incumbent upon executives and managers in charge of an institution to take effective physical security precautions, including the deployment of up to date security appliances. Above all else, they must create and sustain an institutional culture that values and promotes critical thinking, high self-esteem and genuine loyalty to the institution."[65] Without this, vulnerability from within exists, because the greatest threats are insiders "intent upon breaching security to accomplish illicit objectives." [66]

Payment Industry Efforts to Combat Identity Theft Fraud: To Definitively Correspond the User to the Instrument

There are a variety of IT-enabled system security methods, both specific and non-specific to the Payment Industry, that are employed as part of a layered approach to security against ID theft.

Show Me Your ID Please: Identity Authentication Technologies

Generally, identity authentication technologies fall into two broad categories: biometrics and genetic engineering. Biometrics include face recognition, retina scans, fingerprint authentication, voice/speech verification, and handwriting analysis. Face recognition has been studied extensively by the U.S. Department of Defense Counterdrug Technology Development Program Office and the National Institute of Justice. The technology uses a sensor to observe the face and create a biometric signature. A computer algorithm then normalizes the biometric signature making it the same size, view, and resolution as the other signatures in the database. Finally, a matcher compares the normalized signatures and provides a similarity score.[67]

The primary problem with this technology, as with retina scans, is the high cost resulting from the extensive research required to develop it. They are currently regarded, at least in commercial applications, as, "an example of a device whose expenses could outweigh the practicality of its use."[68]

The other identity authentication technology is genetic engineering. Genetic engineering analyzes the DNA components of human fluids and cells. Besides the high cost factor also involved with genetic engineering, this is an example of a technology that has "been met with ethical concerns by individuals worried about the security and privacy of information collected by these devices."[69]

Smart Cards: What is Your Card's IQ?

Smart cards are credit cards that, instead of (or in addition to) a magnetic stripe on the back of the card, have an embedded CPU or electronic chip. These chips "contain 32-kilobyte microprocessors, capable of generating 72 quadrillion or more possible encryption keys, thus making it practically impossible to fraudulently decode information in the chip."[70] According to Tata Consultancy Services, Smart cards offer many advantages over the magnetic stripe technology, including:

- Stores many times more information than a magnetic stripe card.
- Reliable and harder to tamper with than a magnetic stripe card.
- Compatible with portable electronic devices such as phones and personal digital assistants (PDAs), and with PCs.
- Stores highly sensitive data such as signing or encryption keys in a highly secure manner
- Performs certain sensitive operations using signing or encryption keys in a secure fashion.[71]

The primary reason that smart cards have not replaced magnetic stripe cards is that all of the card readers will have to be replaced. MasterCard and Visa will eventually issue deadlines for compliance for embedding chips in cards and processing the cards. Large investments by issuing banks and merchants will be required to comply with these guidelines, so the process is a slow one.

Let's Share: Issuers Clearinghouse

Issuers' Clearinghouse is a joint project between MasterCard and Visa designed to detect fraudulent and high-risk credit card applications.[72] Every MasterCard and Visa application is run through this site to validate

[65] Ibid., 14.
[66] Ibid., 6.
[67] Groves, "Protecting Your Identity," p. 28.
[68] Ibid., 29.
[69] Ibid., 28.
[70] Bhatla, Jej ,Prbhu,Dua, "Understanding Credit Card Frauds" 12.
[71] Ibid.
[72] https://www.merchantconnect.com/CWRWeb/glossary.do?glossaryLetter=i , Viewed October 30, 2004.

and track addresses, phone numbers and Social Security numbers used in credit applications. If multiple applications are processed for any of the same identifying information, the applications are flagged and investigated. This service is one of the oldest forms of fraud detection used by MasterCard.

What's in a Name? NameProtect®

NameProtect® is a MasterCard monitoring service that continuously scans and monitors the Internet. This service watches all gTLD[73] and ccTLDs[74], new registrations and activations. "NameProtect® identifies Web sites, emails, chat rooms and other electronic venues where personal credit card data is published, sold, or traded."[75] Through this program, phishing sites are often shut down within hours of their appearance on the Web. In the case of "Operation Firewall," NameProtect® was an invaluable tool in identifying and then tracking illegal activity.

Case Study: "Operation Firewall." MasterCard International Senior Vice President of Security Risk Services, Sergio Pinon, noticed a suspicious level of activity last November in certain chat rooms and websites known to specialize in credit card and identity document trafficking. He contacted the authorities with his suspicions and worked with them to set up a sting, code-named Operation Firewall. The operation was conducted by the U.S. Secret Service, the Justice Department, Homeland Security, the Royal Canadian Mounted Police, and Europol. It targeted 21 suspects in the United States and seven others in six other countries. Arrests were made on both sides of the Atlantic on October 29, 2004 charging 28 people with stealing, selling, and forging credit card and identification documents including driver's licenses, birth certificates, and foreign and domestic passports. Authorities claimed that the suspects were "responsible for running Web sites that investigators said served as online bazaars for hackers and identity thieves."[76] Investigators say that the suspects bought or sold 1.7 million stolen credit card numbers operating on Internet servers in Belarus, Canada, Sweden, and Ukraine.

Good Fences Make Good Neighbors: General System Security Starts With a Perimeter

The Payment Industry and issuing banks use a layered approach to security—perimeter, app-layer protection, intrusion detection, use of various monitoring tools—because threats are varied, and no environment works as well as it should, in theory.[77] This strategic approach is not unique to the Payment Industry, but rather is standard for all businesses that use a strategic approach to security.

Many industries are now appointing privacy officers who play a strategic role in creating information privacy policies to prevent identity theft. Many of the information manager's responsibilities dovetail with prevention measures: creating retention schedules, properly tracking and filing information, and training staff on information management procedures. The information manager "may assume some or all of a privacy officer's identity protection duties."[78] Information managers and privacy officers should be the ones who step in and help the company understand the laws regarding privacy and security. They also need to train each individual employee on privacy and security. Gary Clayton, Founder and Chairman of the Privacy Council, points out that, "Privacy and security do not work if you do not have top-level buy-in. Information managers might very well be the key people within the organization to help accomplish this."[79]

Increased security to prevent identity theft is one of the key challenges facing MasterCard. Glover T. Ferguson, Chief Scientist with Accenture, offers this advice. "Rather than posing security as a hurdle to overcome, companies should view their customers' privacy needs as an opportunity through which they can differentiate themselves as trust leaders, increase their financial value and even energize entire economies."[80]

[73] Generic Top Level Domains, e.g., ".com" or ".edu"
[74] Country code Top Level Domains, e.g., ".us" for the United States, or ".ca" for Canada
[75] http://www.nameprotect.com/html/services/id_theft/credit_card.html ,Viewed October 30, 2004.
[76] Krebs, Brian, "28 Identity Theft Suspects Arrested in Transatlantic Sting" *The Washington Post*, October 29, 2004.
[77] Bielski, "Striving to Create a Safe Haven Online," 58.
[78] Groves, "Protecting Your Identity," 31.
[79] Ibid.
[80] Myron, "Stolen Names, Big Numbers," 38.

WE'RE FROM THE GOVERNMENT, WE'RE HERE TO HELP: Legislative Efforts to Combat Credit Card Fraud

Identity Theft and Assumption Deterrence Act of 1998

This is the seminal piece of legislation in the fight against identity theft. When The Identity Theft and Assumption Deterrence Act passed in 1998, no court had yet classified a person's identity as tangible personal property.[81] "Nothing in the existing federal statutory scheme specifically prohibits a person from illegally assuming the identity of another individual without first obtaining false documents but with the intent to engage in fraud-related activity."[82] Federal law at the time prohibited the use and transfer of false identification (a felony), but card-not-present crimes committed over the Internet fell through the legal cracks. Key provisions of this legislation included:

- Expressly criminalized identity theft
- Classified private citizens as direct victims of such conduct
- Allowed individual restitution to victims in restoring credit records
- Added identity theft to the U.S. Sentencing Guidelines Manual
- Allowed corporal and financial sanctions by judges at sentencing
- Directed the Federal Trade Commission to establish a centralized clearinghouse to record and track complaints and to provide consumer education
- Instructed the FTC to implement procedures for referring complaints to the three major national consumer-reporting agencies (Experian/TRW, Transunion, and Equifax) and to channel complaints to respective law enforcement agencies.
- Directed the FTC to establish procedures for educating the public[83]

When President Clinton signed the Act into law, he said "as we enter the information age, it is critical that our newest technologies support our oldest values."[84]

[81] Saunders and Zucker, "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption of Deterrence Act" 187.
[82] Ibid., 186.
[83] Ibid., 188-189.
[84] Ibid., 190.

Privacy Act of 2001

Congressional hearings found that the inappropriate display, sale, or purchase of Social Security numbers is a contributing factor to a range of illegal activities including card-not-present fraud and identity theft. "The Privacy Act of 2001 requires that companies obtain a consumer's 'express consent' prior to sharing or selling sensitive information such as Social Security numbers and nonpublic personal financial information."[85]

Consumer Privacy Protection Act (2002)

This legislation placed requirements on data-collection organizations to provide remedies in the case of identity fraud.[86]

Identity Theft Prevention Act (2003) & Social Security Number Misuse Prevention Act (2003)

Between 2002 and 2003, "Reflecting the nation's ongoing concern, at least 50 bills concerning information privacy were introduced in Congress."[87] Each bill further refines previous legislation and attempts to address areas still needing sharpening. These two pieces of 2003 legislation permit legitimate business and government use of Social Security numbers, but ban the sale and display of the numbers "without the expressed consent of the individual." They prohibit the government from displaying Social Security numbers on "public records posted on the Internet or issued to the public through electronic media." They also limit when businesses may require customers to provide their Social Security numbers.[88]

Fair and Accurate Credit Transactions Act of 2003

This legislation is another sweeping attempt to take a variety of steps to stem the increasing growth of card-not-present fraud and identity theft. Provisions include:

- Requires that merchants and bankers truncate account numbers on electronic credit and debit card receipts to print no more than the last 5 digits of the account number.

[85] Heller, Jason, "New Senate Privacy Bill Addresses Personally Identifiable Information" *Intellectual Property &Technology Law Journal*, September 2001, 31-32.
[86] Riordan, "Who Has Your Numbers?" 24.
[87] Ibid.
[88] Ibid.

- Requires credit and debit card issuers to verify the address of the consumer if a request for a new card on an existing account is received within 30 days of a change of address.
- Allows consumers to place "fraud alerts" in their credit files obligating the consumer reporting agencies to verify that the consumer and not a fraudster is opening an account or obtaining a loan.
- Requires the consumer to call only one credit bureau to notify all three.
- Requires regulators to devise a list of "red flag" indicators to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft in order to prevent fraudulent activity before it can cause major damage to a consumer's credit file.
- Allows consumers to request a free credit report once a year to review for inaccuracies or unauthorized activity.[89]

The Identity Theft Penalty Enhancement Act

This is a 2004 law that establishes a new crime of "aggravated identity theft," defined as using a stolen identity to commit other crimes. Convictions for aggravated identity theft carry a mandatory two-year prison sentence.[90]

Anti-Phishing Act of 2004

Introduced by Senator Patrick Leahy in July, this legislation targets the entire scam, all the way from sending the email to creating fraudulent sites. "The Act is smart because it criminalizes the bait—not just successful phishing. It makes it illegal to knowingly send out spoofed email that links to sham websites, with the intention of committing a crime. And it criminalizes the operation of the sham websites that are the locus of the wrongdoing."[91]

Though it's a start, this law will not eradicate the problem of phishing, since many phishers send their emails from other countries, and it is difficult to prosecute offshore crime.

[89] http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=h2622eas.pdf&directory=/diskb/wais/data/108_cong_bills , viewed October 25, 2004.

[90] Ramasastry, Anita, "The Anti-Phishing Act of 2004: A Useful Tool Against Identity Theft" *FindLaw's Writ Legal Commentary*, August 16, 2004, 1-4.

[91] Ibid., 4.

BEST PRACTICES: Don't Be Part of the Problem

Fighting credit card fraud and identity theft are not solely the domain of the credit card systems. Virtually any person, business, or governmental agency can add to the fraud problem if they are not careful in handling and protecting account and private identifying information. Best practices follow a holistic approach, flowing from general guidelines for all industries and government entities, through IT-specific guidelines, down to the individual participants in the credit card systems: consumers, merchants, acquirers and their processors, issuers and their processors, and the payment systems themselves.

Become Part of the Solution! Best Practices for All Industries and Governmental Agencies

As discussed, criminal elements must gain access to account and private identifying information to perpetrate their fraudulent activities. Their jobs are all too easy because of a general lack of control over the data. Businesses and governmental agencies must take actions to protect their employees, customers, and constituents from identity theft. Some specific guidelines are[92]:

- Ask only for the bare minimum amount of information necessary to conduct business. While employers obviously need to keep Social Security number of their employees on file, very few businesses or governmental agencies need the Social Security numbers of their customers or constituents.
- Do not use Social Security numbers as identifiers. Doing so risks putting them in the public domain. Using Social Security numbers for purposes such as drivers' license numbers, insurance identification numbers, or patient record numbers makes it far easier for identity thieves to get the information.
- Regularly check backgrounds of employees who have access to private identifying information, and not just when they are first hired. Simple, periodic criminal records and credit checks will identify employees who may be at higher risks of succumbing to the

[92] "How Can I Protect My Customers From Identify Theft?" Colorado Attorney General: ID Theft Prevention & Information, www.ago.state.co.us/idtheft/clients.htm, viewed November 3, 2003.

financial gains possible from stealing account numbers and private identifying information.

- Define a privacy policy and communicate it to your customers and employees. The policy should describe what information the business or agency collects, what they do to protect it, how they may share the information with other parties, and how they destroy the information when it is no longer needed.
- Protect sensitive paper information like payment card numbers, Social Security numbers, and other private customer identifying data. Secure records in a vault or under lock-and-key. Restrict access only to persons with a legitimate need to know. Shred records when they are no longer needed. Immediately report security breaches to affected customers and law enforcement.
- Conduct a risk assessment for impact from loss or disclosure of business data. Identify areas of concern for the business or agency, and evaluate the likely amount of damage or disruption based on the assigned level of risk. Table 2 depicts example areas of concern, and typical damage assessments for three levels of risk: low, medium, and high. Once completing the risk assessment, the business or agency should design record retention policies and physical access controls that are appropriate based on the assessed risks of loss or disclosure. [93]

Area of Concern	Low	Medium	High
Business Disruption	-	Moderate	Major
Legal impact	-	Minor	Major
Financial Impact	-	Minor	Major
Health & Safety Impact	-	-	Threatened
Effort to Restore	Easy	Moderate	Significant

Table 2: Example Risk Assessment areas of concern and damage assessment

You Only Thought You Knew It All Already?! Best Practices For IT Practitioners

Since most businesses and governmental agencies these days use IT-based solutions for record keeping and customer relationship management, it is incumbent on IT organizations to implement and follow best practices for protecting the enterprise from attacks. PC Magazine[94] and the Carnegie Mellon Software Engineering Institute's (SEI) CERT® Coordination Center[95] outline the following best practices for IT security:

- Use physical firewall devices and anti-virus, anti-spyware, and access control software to protect networks and computers from external attacks. While each type of protection alone provides some measure or security, all are needed to fully secure networks, servers, and personal computers.
- Keep operating system and security software up-to-date with the latest security patches from the software vendors.
- Define policies for strong passwords and require users to change them frequently. Discourage passwords that are too easily guessed, such as those based on easily collected personal information, but don't require passwords so difficult to remember that employees must write them down. Replace default passwords and disable guest accounts too.
- Monitor network, firewall, web server and PC security logs for signs of any abnormal behavior. A higher than usual number of invalid user id or invalid password log entries might indicate someone is attempting to hack into the network or server.
- Frequently monitor security information websites for breaking information about new threats and best practices (e.g., CERT® Coordination Center).
- Protect sensitive electronic information like private customer identifying data and account numbers. Restrict data access rights to only those persons and systems with legitimate needs to know, and consider encrypting sensitive information housed in databases.
- Segregate sensitive data on separate servers from web servers to provide an additional layer of protection against external attacks. Otherwise, a hacker who defeats the security

[93] "Network Security Policy: Best Practices White Paper," Cisco Systems, www.cisco.com/warp/public/126/secpol.html, 2, viewed November 2, 2004.

[94] "Webserver Security Best Practices", *PC Magazine*, www.pcmag.com/article2/0,4149,11525,00.asp, viewed November 2, 2004.

[95] CERT® Security Improvement Modules, CERT® Coordination Center, www.cert.org/security-improvement, viewed November 2, 2004.

on your web site has immediate access to your database. Keeping the data separate requires hackers to work harder and longer, and may give you just enough time to detect their activities.

Only You Can Prevent Fraud! Best Practices For Consumers

A diligent, informed, aware consumer can take responsibility for protecting himself or herself from many low-technology fraud opportunities. Suggestions from MasterCard and Canada's public safety watchdog include:[96,97]

- Only give payment account numbers or personal identification information to companies you have contacted
- Challenge businesses that ask for personal identification information about why they need to know
- Avoid saying information over the phone when others may hear
- Do not carry unnecessary payment cards or identification papers (e.g., Social Security card, birth certificate) in your wallet or purse
- Do not use SSN for your driver's license or other identification cards
- Keep track of receipts for payment card transactions
- Shred receipts and account statements having full account numbers, and the unsolicited credit card and loan applications you receive in the mail
- Cancel unused credit card accounts
- Keep a list of all of your payment card account numbers along with their issuers' names and contact numbers so you can cancel them quickly if lost or stolen
- Use firewall, anti-virus, and anti-spyware software on your PC
- Keep your PC operating system and security software up-to-date with latest security patches from your vendors
- Be suspicious of emails and websites requesting private information
- Verify URLs and make sure websites are secure before entering account numbers and personal private identifying information
- Be careful when locating websites through search engines to ensure you have found the legitimate site
- Call the company if you are unsure of the validity of a website

There's More to Business Than Collecting Bags of Money! Best Practices For Merchants

Merchants are charged with employing the latest IT-enabled cardholder authentication technologies and applicable credit card system rules to ensure secure financial transactions. Examples of these include:[98]

Card Present

- Check that the embossing on the card extends into the hologram
- Check the hologram and indent printing
- Compare the signature on the card to the one on the sales draft
- Check that the magnetic strip appears authentic
- Call for a "Code 10" authorization if something doesn't "feel" right

Card-not-Present

- Use address verification systems to check the account holder's billing address
- Implement SecureCode and Verified by Visa services
- Include card verification values/codes in authorization messages (but do not store them in your database)
- Require complete customer contact and payment information before completing an order
- Process transactions in real-time

[96] "Best Practices for Preventing Online Identity Theft," Public Safety and Emergency Preparedness Canada, www.ocipep-bpiepc.gc.ca/opsprods/info_notes/IN04-002_e.asp. Viewed November 2, 2004.

[97] "Tips for Preventing Payment Card Fraud," MasterCard International, www.mastercardinternational.com/newsroom/security_risk.html, viewed October 22, 2004.

[98] "Preventing Fraud: Fighting Fraud is a Shared Responsibility," MasterCard International, www.mastercardmerchant.com/preventing_fraud, viewed October 28, 2004.

- Keep the customer on the website until the payment card is authorized and the sale is completed
- Monitor international transactions
- Employ rules-based systems to screen and detect suspicious order activity
- Maintain negative databases of fraudulent orders and offenders, and positive databases of trusted returning customers
- Adopt MasterCard's Best Practices for eCommerce websites
- Have a Site Data Protection audit done on your eCommerce website

Protect Yourself From Your Merchants! Best Practices For Acquirers and Acquiring Processors

Acquirers and their processors are accountable and liable for the actions of their sponsored merchants. In addition to implementing the industry and IT best practices described above, acquirers should consider adopting the following best practices to protect themselves and their merchants:

- Provide merchants with access to security features developed by the credit card systems, and compel them with contracts and pricing incentives to use the features. Security features such as MasterCard's Address Verification Service and SecureCode go a long way to protect merchants and prevent fraudulent activity.
- Monitor merchant deposit velocity for unexpected increases in deposits. While a significant spike or increase in a merchant's deposits may be due to nothing more than a sale or improving business conditions, it could indicate a merchant who has an employee who is colluding to commit fraud. Acquirers should consider freezing funds for excess deposits until they can investigate the suspicious activity.
- Check and report each merchant's termination history. Before contracting with a new merchant to begin accepting credit card transactions, Acquirers must check out the merchant's history using MasterCard's Merchant Online Status Tracking system. Any "hits" must be investigated. Acquirers also must report merchants who were terminated for cause, such as for violating association rules, or for having excessive fraudulent activity.

The Last Line of Defense: Best Practices For Issuers and Issuing Processors

Issuers and their processors are accountable and liable for the actions of their cardholders. In addition to implementing the industry and IT best practices described above, issuers should consider adopting the following best practices to protect themselves and their cardholders:

- Monitor cardholder purchase and cash velocity for drastic changes. Significant increases in the number of uses or the accumulated spending amount over a short period of time may indicate that a card was lost, stolen, or was otherwise compromised. Issuers should contact the cardholder to ensure the uses are legitimate, and consider temporarily blocking a card if they are unable to contact the cardholder in a reasonable amount of time.
- Use behavioral model/neural network software such as MasterCard's RiskFinder product to detect fundamental changes in cardholders' behaviors. As with velocity changes above, investigate significant changes and consider temporary blocks to mitigate exposure.

Protect Your Brand! Best Practices For Payment Companies

Payment companies are the ultimate guarantors of the credit card systems. Companies like MasterCard, Visa, and American Express work hard to protect consumer confidence in their brands. Credit card fraud and identity theft represent serious challenges and could quickly erode consumer confidence in the system if left unchecked. In addition to implementing the industry and IT best practices described above, the payment companies adopt the following best practices to protect themselves and their constituents:

- Monitor to detect shifts in types and volumes of fraudulent activity. The dynamics of fraudulent activity are constantly changing. Criminal elements are adept at finding and exploiting new weaknesses. The pervasiveness of information sharing on the Internet permits information about new weaknesses to be quickly broadcast to hackers and crime organizations. New schemes for attacks start with a trickle of activity, and quickly change to a deluge.

- Cooperate with each other to conduct research to innovate new fraud detection and prevention mechanisms. Continue research on emerging technologies that authenticate the card, the account number, and the cardholder to the card.
- Continue to create, refresh and enforce security standards to adapt to the dynamic nature of fraud. Adaptation is the key to survival of the fittest. The payment companies that are best able to adapt will shed attackers, who then will focus on the weaker victims.

CONCLUSION

Fraudulent credit card activities present unique challenges for MasterCard and other credit card companies, financial institutions that issue and process credit card transactions, merchants, and consumers. Criminals find creative ways to capture private credit cardholder account and identification information, and the credit card industry spends millions of dollars annually searching for ways to detect and prevent them. MasterCard International has licensed security measures designed to combat the significant threats posed by card-not-present and identity theft credit card fraud, and has corporate functions aimed at the detection and capture of emerging types of credit card fraud. Fighting credit card fraud is also the responsibility of the cardholder, however. To successfully counter the growing threats posed by credit card fraud and identification theft, it is critical that every participant in the credit card transactional flow assume responsibility for the protection and monitoring of personal and financial information.