Credit Card Fraud

CREDIT CARD FRAUD

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.
The cost of credit card fraud reaches into billions of dollars annually. In 2006, fraud in the United Kingdom alone was estimated at £428 million, or US$750-830 million at prevailing 2006 exchange rates.

Origins

The fraud begins with either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder, the merchant or the bank, at least until the account is ultimately used for fraud. A simple example is that of a store clerk copying sales receipts for later use. The rapid growth of credit card use on the Internet has made database security lapses particularly costly; in some cases, millions of accounts have been compromised.

Stolen cards can be reported quickly by card holders, but a compromised account can be hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The card holder may not discover fraudulent use until receiving a billing statement, which may be delivered infrequently.

Stolen cards

When a credit card is lost or stolen, it remains usable until the holder notifies the bank that the card is lost; most banks have toll-free telephone numbers with 24-hour support to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on that card up until the card is cancelled. In the absence of other security measures, a thief could potentially purchase thousands of dollars in merchandise or services before the card holder or the bank realize that the card is in the wrong hands.

In the United States, federal law limits the liability of card holders to $50 in the event of theft, regardless of the amount charged on the card; in practice, many banks will waive even this small payment and simply remove the fraudulent charges from the customer's account if the customer signs an affidavit confirming that the charges are indeed fraudulent. Other countries generally have similar laws aimed at protecting consumers from physical theft of the card.
The only common security measure on all cards is a signature panel, but signatures are relatively easy to forge. Many merchants will demand to see a picture ID, such as a driver's license, to verify the identity of the purchaser, and some credit cards include the holder's picture on the card itself. However, the card holder has a right to refuse to show additional verification, and asking for such verification may be a violation of the merchant's agreement with the credit card companies. Self-serve payment systems (gas stations, kiosks, etc.) are common targets for stolen cards, as there is no way to verify the card holder's identity. A common countermeasure is to require the user to key in some identifying information, such as the user's ZIP or postal code. This method may deter casual theft of a card found alone, but if the card holder's wallet is stolen, it may be trivial for the thief to deduce the information by looking at other items in the wallet. For instance, a U.S. driver license commonly has the holder's home address and ZIP code printed on it.
Banks have a number of countermeasures at the network level, including sophisticated real-time analysis that can estimate the probability of fraud based on a number of factors. For example, a large transaction occurring a great distance from the card holder's home might be flagged as suspicious. The merchant may be instructed to call the bank for verification, to decline the transaction, or even to hold the card and refuse to return it to the customer.

Compromised accounts

Logistica Solutions Inc., 1251 N Jefferson St, Anaheim, Ca 92807, USA, (714) 238-3209
http://www.ecomstor.com - http://www.interpristor.com - info@ecomstor.com

Credit Card Fraud

Card account information is stored in a number of formats. Account numbers are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in machine readable format. Fields can vary, but the most common include:

- Name of card holder
- Account number
- Expiration date
- Verification/CVV code

Many Web sites have been compromised in the past and theft of credit card data is a major concern for banks. Data obtained in a theft, like addresses or phone numbers, can be highly useful to a thief as additional card holder verification.

Mail / Internet order fraud

The mail and the Internet are major routes for fraud against merchants who sell and ship products, as well Internet merchants who provide online services. The industry term for catalog order and similar transactions is "Card Not Present" (CNP), meaning that the card is not physically available for the merchant to inspect. The merchant must rely on the holder (or someone purporting to be the holder) to present the information on the card by indirect means, whether by mail, telephone or over the Internet when the cardholder is not present at the point of sale.
It is difficult for a merchant to verify that the actual card holder is indeed authorizing the purchase. Shipping companies can guarantee delivery to a location, but they are not required to check identification and they are usually are not involved in processing payments for the merchandise. A common preventive measure for merchants is to allow shipment only to an address approved by the cardholder, and merchant banking systems offer simple methods of verifying this information.

Additionally, smaller transactions generally undergo less scrutiny, and are less likely to be investigated by either the bank or the merchant, since the cost of research and prosecution usually far outweighs the loss due to fraud. CNP merchants must take extra precaution against fraud exposure and associated losses, and they pay higher rates to merchant banks for the privilege of accepting cards. Anonymous scam artists bet on the fact that many fraud prevention features do not apply in this environment.

Merchant associations have developed some prevention measures, such as single use card numbers, but these have not met with much success. Customers expect to be able to use their credit card without any hassles, and have little incentive to pursue additional security due to laws limiting customer liability in the event of fraud. Merchants can implement these prevention measures but risk losing business if the customer chooses not to use the measures.

Account takeover

There are two types of fraud within the identity theft category, application fraud and account takeover.
Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may create counterfeit documents.

Account takeover involves a criminal trying to take over another person's account, first by gathering information about the intended victim, then contacting their bank or credit issuer — masquerading as the genuine cardholder — asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent. The replacement card is then used fraudulently.

Some merchants added a new practice to protect consumers and self reputation, where they ask the buyer to send a copy of the physical card and statement to ensure the legitimate usage of a card.

Logistica Solutions Inc., 1251 N Jefferson St, Anaheim, Ca 92807, USA, (714) 238-3209
http://www.ecomstor.com - http://www.interpristor.com - info@ecomstor.com

Credit Card Fraud

Skimming

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant, and can be as simple as photocopying of receipts. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time.

Skimming is difficult for the typical card holder to detect, but given a large enough sample, it is fairly easy for the bank to detect. The bank collects a list of all the card holders who have complained about fraudulent transactions, and then uses data mining to discover relationships among the card holders and the merchants they use. For example, if many of the customers used one particular merchant, that merchant's terminals (devices used to authorize transactions) can be directly investigated. Sophisticated algorithms can also search for known patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe in cases of compromise, ranging from large fines to complete exclusion from the merchant banking system, which can be a death blow to businesses such as restaurants which rely on credit card processing.

Carding

Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a Web site subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the bank's attention. A website known to be susceptible to carding is known as a card able website.

In the past, carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which valid accounts were. Another variation would be to take false card numbers to a location that does not immediately process card numbers, such as a trade show or special event. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or the card's expiry date, as well as the more prevalent use of wireless card scanners that can process transactions right away. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing.

A set of credit card details that has been verified in this way is known in fraud circles as a phish. A carder will typically sell data files of phish to other individuals who will carry out the actual fraud. Market price for a phish ranges from US$1.00 to US$50.00 depending on the type of card, freshness of the data and credit status of the victim.

Profits, losses and punishment

The examples and perspective in this article or section may not represent a worldwide view of the subject.
Please improve this article or discuss the issue on the talk page.

Losses

Please help improve this article or section by expanding it.
Further information might be found on the talk page or at requests for expansion. (August 2007)
U.S. federal law can hold the cardholder victim responsible for up to $50. Merchants in high-risk industries such as

Logistica Solutions Inc., 1251 N Jefferson St, Anaheim, Ca 92807, USA, (714) 238-3209
http://www.ecomstor.com - http://www.interpristor.com - info@ecomstor.com

unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly. These higher costs are then passed onto the customer. The FBI's Financial Report to the Public for 2007 report losses of $52.6 billion, affecting 9.91 million Americans.

Credit card companies

This section may require cleanup to meet Wikipedia's quality standards.
Please improve this article if you can (May 2008).

In the case of fraud, the merchant and not the credit card company pay the full cost of the fraud plus a chargeback fee or the merchant's chargeback insurance covers it. In addition credit card companies have to pay for preventing fraud while maintaining a good customer experience. Online merchants have the ability to sign up for services offered by Visa and Mastercard i.e. "Verified By Visa" or "MasterCard SecureCode" to prevent being "chargedback" for fraud transactions. In addition merchants often do not take adequate measures to protect their websites from fraud attacks.
Credit card merchant associations, like Visa and MasterCard, and their member banks receive profit from transaction fees, with the lowest known in the industry as the discount, mid-qualified, and non-qualified rates. The discount rate is a percentage of the amount of the transaction, with typical merchants receiving discount rates in the range of 2% to 4%. Merchant associations are thus motivated to pursue policies which increase the aggregate amount of money transferred by their systems. Many merchants believe this pursuit of revenue generation reduces the incentive for credit card banks to implement procedures to reduce credit card crime, particularly since the cost of investigating fraud is usually higher than the cost of a write-off. However, merchant associations are not assuming these costs; they are instead passed on to merchants as "chargebacks". This result in substantial additional costs: not only has the merchant been defrauded for the amount of the transaction, but he is also obligated to pay a chargeback fee, and to make matters worse, the merchant is not even reimbursed for his transaction fees.

Merchants have begun to request changes in State and Federal Laws to protect consumers and merchants from fraud, but the credit card industry has opposed many of the requested laws. In many cases, merchants have little ability to fight fraud, and must simply accept a certain percentage of fraud as a cost of doing business.
Because all card-accepting merchants and card-carrying customers are bound by contract law, according to the agreements they sign with their processing / issuing banks, respectively, State and Federal law has a smaller role in preventing merchants from being tricked. Payment transfer associations enact regulatory changes, and issuing / acquiring banks, merchants, and cardholders are contractually bound to these new regulations.

Merchants

The merchant loses the goods or services sold, the payment, the fees for processing the payment, any currency conversion commissions, and the chargeback penalty. For obvious reasons, many merchants take steps to avoid chargebacks — such as not accepting suspicious transactions. This may spawn collateral damage, where the merchant additionally loses legitimate sales by incorrectly blocking legitimate transactions.

Criminals

In the U.S., persons that commit credit card crime largely go unpunished and repeatedly victimize consumers and businesses. The Secret Service handles crimes involving the U.S. money supply; they have a limit of $150,000 before investigating each crime. Most credit card criminals know this and keep purchases from any one business below $150,000. Credit card fraud can be reported to the Federal Trade Commission (FTC) and to local and regional authorities. It is the standing policy of the FTC not to investigate reports where the value of fraud does not exceed $2000. Local law enforcement may or may not further investigate a credit card fraud, depending on the amount, type of fraud, and where the fraud originated from.

The Cardholder Information Security Program (CISP) was a program established by Visa USA to ensure the security of

Logistica Solutions Inc., 1251 N Jefferson St, Anaheim, Ca 92807, USA, (714) 238-3209
http://www.ecomstor.com - http://www.interpristor.com - info@ecomstor.com

cardholder information as it is being processed and stored by merchants and service providers.
CISP has since been superseded by the PCI Data Security Standard

Logistica Solutions Inc., 1251 N Jefferson St, Anaheim, Ca 92807, USA, (714) 238-3209
http://www.ecomstor.com - http://www.interpristor.com - info@ecomstor.com