Fraud Prevention
Issuer's Best Practice Guide

Rev. March 2011

Notices

Disclaimer

FIS uses reasonable efforts to ensure the accuracy of the material described in this manual. This manual is current only through the revised date. Thereafter, changes to FIS's systems, programs, and procedures may occur that are not referenced in this manual. Such changes will be communicated to the financial institution via bulletins. In addition, from time to time, FIS may make updates to this manual available to the institution.

FIS makes no warranty, express or implied, with respect to the quality, accuracy or completeness of this manual or the products it describes. FIS makes no representation or warranty with respect to the contents of this manual and specifically disclaims:

- any implied warranties of fitness for any particular purpose; and
- liability for any direct, indirect, incidental or consequential, special or exemplary damages, including but not limited to, lost profits resulting from the use of the information in the manual or from the use of any products described in this manual.

Data used in examples and sample data files are provided for practice and illustration purposes only. Any similarities to real persons or companies in any examples or illustrations are entirely coincidental.

Before commencing use of reference materials provided by FIS, the institution should review its entire Financial Institution Service Agreement with FIS to familiarize itself with all of the terms of the Agreement. The institution should specifically review the contractual obligations listed below.

Institution's Responsibilities

The financial institution is solely responsible for compliance with:

- all laws, rules, and regulations applicable to all aspects of the operations of the Visa and/or MasterCard programs;
- usury laws;
- the Truth-In-Lending, Fair Credit Reporting, Equal Credit Opportunity, and Electronic Funds Transfer Acts;
- all state laws and regulations regardless of whether the financial institution uses any forms or other materials supplied by FIS.

The financial institution has already acknowledged that either it possesses a copy of the Visa and MasterCard by-laws, rules, and regulations, or it knows that it may receive a copy of each by requesting them in writing from Visa and MasterCard or FIS, and paying the applicable fees.

Confidentiality

The financial institution has agreed to hold as secret and confidential information, reports, plans, cardholder lists, documents, drawings, writings, samples, know-how, and other proprietary material received from FIS (Confidential Information). Confidential Information provided by FIS remains the property of FIS. The financial institution must restrict access to Confidential Information received from FIS to those employees and persons in the organization who need to know such Confidential Information in order to fulfill their obligations. The contents of this manual and other information provided by FIS are deemed to be Confidential Information.

The institution should review the Financial Institution Service Agreement with FIS if it has any questions regarding the above. For any questions of a legal nature, the institution should consult legal counsel.

Table of Contents

Overall Best Defense

Today's changing environment plays a large role in the increase of card fraud. Worldwide electronic information sharing, electronic data storage, online purchasing, and frequency and ease of card usage increase the chances for all financial institutions and their cardholders to be victims of card fraud.

Awareness of fraud trends, knowledge of risk management options available to curb fraud, and always being on the lookout for fraud indicators are key to reducing a financial institutions loss due to card fraud. Thinking in terms of "when fraud happens" should replace the attitude of "if fraud happens".

A well-developed fraud prevention program to adequately address the changing nature of fraud and to help reduce the risks associated with fraudulent activity may help institutions meet these goals.

The following best practice tips and guide are designed to help you begin incorporating this new way of thinking in terms of fraud and its affect on your financial institutions and cardholders into your daily processes.

Best Practices

FIS recommends the following best practices.

Keep current on the latest fraud trends affecting the industry.
This will give you the ability to identify fraud attempts against your account(s) in the early stages so you can then choose to use the available tools that fit the situation to reduce the impact of the situation on your financial institution. Being cognizant of fraud trends also may allow you to be a step ahead of a potential fraud attack by taking action to protect your institution based on the patterns reported by other industry members.

Be aware of the risk management products available to issuers and merchants.
It is necessary to have a good understanding of how risk products work and to utilize all the tools that may be effective to your fraud prevention efforts. There is no one risk product that will stop all fraud, but a combination of options can greatly reduce your risk levels and fraud losses.

Be familiar with the various fraud types and how to properly identify them.
This knowledge is useful when analyzing a fraud situation to distinguish the magnitude of fraud that is occurring, reporting the fraud to the proper authorities, and deciding the actions to take to reduce the loss to your financial institution.

Educate your financial institution's staff about foreign fraud.
The occurrence of fraud in foreign countries has increased significantly with the world market situation we operate in today, whether your cardholder has been to a foreign country or not. It is in an institution's best interest to be able to recognize the common characteristics of foreign fraud, to be aware of what is available to protect your institution, and who to report fraud to when it does occur.

Incorporate an authorization monitoring process into your daily routine.
Along with utilizing Falcon, we suggest you include a manual report monitoring process that can help detect fraud patterns that may be evident to the human eye and mind but not yet common enough to generate a high score in a neural network system.

Develop a policy for addressing Visa CAMS and MasterCard alerts.
Train your staff to analyze the information provided in notices from Visa CAMS and MasterCard alerts documents. This will give you the confidence to choose the best line of defense based on the alert at hand.

Realize the direct impact of Phishing scams to your cardholders and institution and know how to recognize these attempts.
One of the latest schemes used to deceive cardholders today is "Phishing". Perpetrators communicate directly with their potential victims via email, hoping to obtain detailed personal data including card information. Cardholder awareness can be an effective prevention tool for this type of fraud scam.

Blocking and reissuing cardholder's cards.
Be aware that there will be situations that require your staff to make a decision to block a cardholder's account in order to avoid losses. Setting guidelines to determine when the institution, due to potential fraud, will block accounts and what steps will be taken to notify the cardholders affected will allow staff to make this decision with confidence.

Use the resources available to you to help with your institution's education efforts.
Many resources are available to keep you informed and up to date about fraud, to offer the opportunity to share information, to report fraud trends, to research fraud situations and to answer your questions about preventative processes and measures. The difficult part is knowing where to find this information.

Fraud Trends

As technology and society change, so do the fraud trends that emerge in the card industry. The industry is usually in a reactionary mode when dealing with fraud issues, because it is often hard to predict which systems will be attacked in a new fraud scheme.

The most successful fraud attacks generally involve the discovery of a system or software weakness, which the criminals will exploit until a fix is devised to prevent the problem from occurring. The widespread use of the Internet has fueled much of today's fraud trends.

Debit card fraud has increased because so many new card programs have been launched in the past few years as consumers become more comfortable with the convenience provided by using debit cards instead of paper checks. Our monetary transactions are driven by the merchants' need for speed and accuracy, which debit cards bring to the market. Debit cards are the choice medium for today's consumers when buying and selling goods and services. The exposure created through continual use has made debit cards an open target for fraud. Since debit cards move through the card industry much like credit cards, criminals find them equally attractive.

Organized cyber fraud rings have developed spanning many geographic locations, social structures, and ethic groups. Because the members of these groups do not need to know each other personally to engage in organized crime these loosely knit gangs can come into being and disband at a moments notice. By combining their efforts and use of the Internet, these cyber criminals can compromise millions of cardholders all over the world.

Foreign fraud has exploded over the past year due to data compromised at merchant's sites and then resulting in large losses to skimmed counterfeit fraud. Merchant data compromises, data stolen from universities, and skimmed data sold by dishonest employees have been the drivers for much of the foreign fraud. New Internet based schemes such as "phishing" and "pharming" can be operated from foreign web sites or web connections, which result in fraud.

Merchant data compromises are not only linked to foreign fraud, many issuers have suffered losses from runners within the United States and found the account data seems to be connected to a given alert regarding a merchant compromise. This trend continues to plague the industry. Because compromises can take place in so many different ways, it has been hard for the industry to control this outbreak of crime against merchants. Perpetrators to accomplish their corrupt goals have used everything from direct use of stolen passwords to wireless interception of data.

Savvy criminals who try to trick the consumer into giving away their personal identifying information or account data have also directly targeted cardholders. Consumer "phishing" and pharming tools exist, along with many other Internet based schemes that set out to deceive the consumer. For this reason, cardholder education is a necessary element in building a good fraud prevention plan.

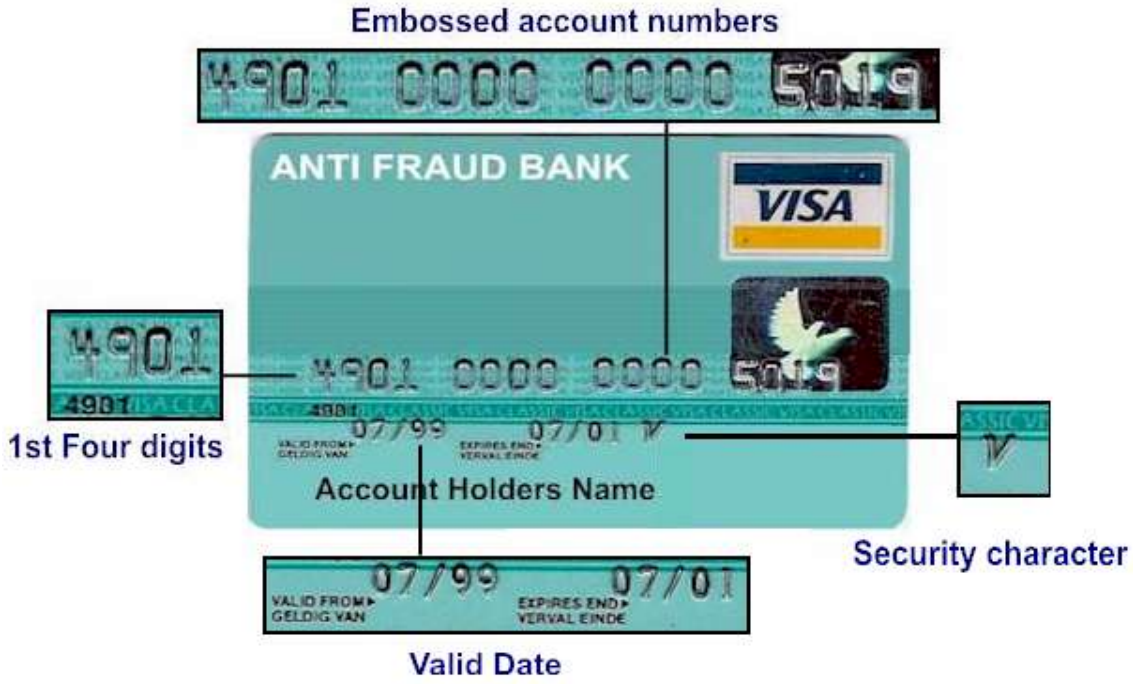
Risk Management Products

The card industry has some risks management products that are designed to help both issuers and merchants combat fraud. For the merchant the card security features are effect in face-to-face transactions and address verification service helps in card not present situations, together they are two primary tools designed to limit the criminal's ability to deceive the merchant through fraud.

Card Security Features

In today's society, Credit / Debit cards have become and everyday household item. All too often in a fast paced environment a counterfeit card is passed around without even being noticed! Few people take the time to validate all the security features designed into every card. Visa and MasterCard established strict design specifications for the production of their cards, which help reduce the criminal's opportunity to produce counterfeit cards. Below are a few pointers on what to look for when processing a card-present transaction.

Sample Card:



The Account number

The last four numbers of the account listed on the receipt should always match the last four numbers on the card. The account number should belong to the

issuing financial institution shown on the card. The account number embossed on the card should match the account contained in the magnetic stripe data.

The Signature Panel

The signature panel on the back of the card should display an angled, repeated pattern of the words "Visa" or "MasterCard" and either the complete, or a portion of the 16 digit card number. Also, along with the CVV2 and the CVC2 codes on the signature panel as well.

A blank signature panel is a clear sign of an altered card. If the over-print pattern in the signature panel has been altered (For example by erasure) the word "Void" will be exposed.

The Hologram

A hologram is a laser-created, three-dimensional image that is placed on Visa and MasterCard cards as an additional card validation tool.

Visa should have a three-dimensional dove hologram that should reflect light and seem to change as you rotate the card.

MasterCard should also have a three dimensional hologram with interlocking globes that should reflect light and seem to change when you rotate the card. The word "MasterCard" is printed repeatedly in the background of the hologram. The letters "MC" are micro-engraved around the two rings.

The Magnetic Stripe

The Magnetic stripe should appear smooth and straight, with no signs of tampering. This feature houses the card data that will be read by the merchant's terminal at the point of sale. The magnetic stripe has three tracks for data that can be read by the right equipment.

Track one has the account number, cardholder's name, expiration date, CVV and CVC 1 codes, and the Pin offset code. Track two has the same data, as track one except the cardholder's name and track three is usually blank.

The Visa Logo

Another counterfeit deterrent that Visa offers on their cards is the micro-printed information around the Visa logo. Some counterfeit cards will have either no micro printing or a dotted line in place of the micro printing.

The MasterCard Debit Card

MasterCard offers a special hologram for debit cards. The word "Debit" appears in the hologram.

For more information on card security features please refer to Chapter 2 of the Fraud Prevention Guide.

Address Verification Service

One control that a card not present merchant has is the address to which the merchandise is shipped. This single factor completes the sale and gives the customer the goods that have been ordered.

Address Verification Service allows the merchant to confirm that the shipping address for the purchase corresponds to the home or billing address on the card file. Although this cannot guarantee that the cardholder is making the purchase, it does reassure the merchant that the goods will be delivered to a known address that is associated with this customer.

Expiration Mismatch

Expiration mismatch is a system feature that allows the merchant to compare the expiration date within the magnetic stripe data for swiped transactions or the date keyed into the system for manually keyed transaction to the actual card expiration date contained in the master file as part of the transaction authorization process.

If the date submitted during the authorization does not match the file date, the transaction is declined. In some cases, perpetrators have access to number generating software that can create mode 10 account numbers. This number may or may not be active or valid. Once the number has been validated, the card expiration date must then be guessed in order to complete a transaction where expiration mismatch is enforced.

Name Matching

Name match technology has recently been introduced to reduce counterfeit skimming when the merchant sends the full track one data to be verified. The name of the cardholder in the transmitted data must match the name on record on the master file. Often perpetrators will change the name to match their fake ID or to better fit their personal profile. Name matching requires the original cardholders name in order to authorize the transaction.

Verified By Visa and MasterCard Secure Code

Verified by Visa and MasterCard Secure are programs designed to help protect Internet shoppers and merchants from fraud. In these programs, the customer goes online and creates a personal password. When the customer makes payments online with merchants that have this product in the customer will be asked to use this password for additional identification.

Card Verification Value 2 (CVV2) and Card Verification Code 2 (CVC2)

On the back of every card there is a unique three digit number that can be used to validate that a customer has the card in their possession. The code is created by a special formula and is only used on one card. This value can be requested by merchants or service providers to assure them that the card is with the customer they are dealing with at the time. This security feature is designed to aid in card not present transactions.

For information to help your institution evaluate its key fraud system parameter settings and practices, reference the monthly Fraud Assessment Report found in E-Reports. (TBS System – CPFRDRPT-01; Base 2000 System – BPFRDRPT-01; Pass-Through System – PD508; EFT System – PM508)

Fraud by Fraud Types

When working with the different fraud types issuers should be prepared to act appropriately to avoid losses on their card programs. Six fraud types are used to cover the various patterns created in a fraud situation. These fraud types are lost/stolen, counterfeit/skimming, never received issue (NRI), fraudulent applications, account takeover (ATO), and card not present (CNP) fraud. Understanding the basics of each fraud type may help issuers better prepare their organization to service their customers in each situation and to control their losses.

For more detailed information on fraud types, refer to Chapter 3 of the Fraud Prevention Guide.

Lost/Stolen Cards

Lost/stolen card fraud must be controlled with the partnership of your cardholders. This fraud type is characterized by the cardholder's claim that they no long have possession of a card that they once possessed and when the fraudulent activity occurs, the cardholder does not have the card because an unauthorized user is using the original card.

Lost/stolen cards generally show three types of purchasing patterns because the assumption is that the perpetrator wants to use all the available funds as quickly as possible before the cardholder discovers that the card is missing, reports the card, and the card is blocked.

The perpetrator may make several smaller purchases that generate excessive volume on the account. The card may be used to make a few very large purchases to create less risk of exposure by the perpetrator. Thirdly, the card may be used for multiple cash advances, large or small, to maximize the cash value that can be gained from the card.

A neural network such as Fraud Alert Management or daily account monitoring may detect lost/stolen cards when the volume of transactions and/or dollar amounts differs from the normal cardholder-spending pattern. In these cases, the activity on the account has prompted the investigator to contact the cardholder who was not aware that they did not have possession of the card until the contact was made.

The cardholder making a report to the card issuer or FIS claiming that the card has been misplaced may also detect lost/stolen cards.

Issuers can help prevent the losses due to lost /stolen cards by having a good neural network in place and keeping cardholder contact information current. Monitoring the daily authorizations on your card program may help the issuer to detect an abnormal change in spending; transaction location, or increased cash advances activity on the account. A call to the cardholder will then confirm the cards status. When cards are reported to the issuer directly by the cardholder, issuers should make sure that the proper assistance is available 24/7. Cardholders should be given up-to-date telephone numbers and encouraged to not delay their reporting to standard business hours.

Special incentives or reminders may serve to motivate cardholders to update their personal information and to carefully handle their cards. Issuers should encourage cardholders to file a police report in the community where the card was lost or stolen.

Cardholders should be asked to report their version of how the card became missing and if the PIN number or any other identification documents were with the card. Issuers should review all lost/stolen card claims for possible indicators of cardholder abuse.

Counterfeit/skimming

Counterfeit fraud is the use of an altered or illegally reproduced card and the use of replicated magnetic stripe data that has been illegally obtained for unauthorized purchases. In these cases, the cardholders will have possession of their cards. The transactions will come through the systems with a POS entry mode of 90, 80, 02, or 05.

This type of fraud can occur by the use of an electronic device that reads and copies magnetic stripe data. Account information may be taken directly from a merchant's data stream where the card was used for a legitimate transaction or generated by the use of software program called Credit Master or Credit Wizard.

These software programs allow the perpetrator to quickly formulate mode 10 account numbers that may be open on any BIN entered into the program. These account numbers produced by Credit Master must be tested to see if the numbers are associated with active accounts.

The expiration date and other security features such as, CVV/CVC 1 and CVV/CVC 2 must be guessed or created before the number can be used in any merchant transaction. Therefore, this method of counterfeiting is less like to occur since the perpetrator lacks the ability to reproduce these codes. Key entered transactions or card not present transactions may result in a Credit Master situation and the issuer will see account testing.

A neural network that identifies the fraudulent activity of the perpetrator best detects counterfeit fraud. The "testing" pattern used to validate the card data before it is sold or used by the perpetrator may also allow issuers to detect counterfeit fraud. This detection can be accomplished by checking daily authorization reports for any known testing pattern involving specific merchants, MCC codes, or dollar amounts. Having low or even dollar amounts and occurring within a short time period characterize test authorizations. Although there may be exceptions to this pattern, test authorization usually never post to the account.

Recent counterfeit schemes have involved the use of foreign merchants. Because the Internet allows the perpetrator to email data easily without any contact with the other party this is believed to be how many United States issuers have been victimized by counterfeit fraud from numerous foreign countries. Many issuers have chosen to apply parameter blocks that limit or restrict transactions from certain countries where fraud has occurred or where their accounts have experienced account testing. Issuers should work with their client relation's representatives to implement country blocks on the FIS authorization system.

The use of neural network systems and daily account authorization activity monitoring are the best defense against counterfeit fraud. A neural network with rule-writing capability is most helpful because these rules can be changed once a new pattern has been discovered. Systems such as name matching that validate track 1 data against a master file may reduce this type of fraud when the merchant transmits full track 1 data.

Counterfeit fraud that impacts a large group of accounts may have resulted from a common point of purchase. Issuers are encouraged to review transaction data on fraud accounts to see if the cardholders used a common merchant or a series of merchants. Any findings that indicate a security breach at a merchant site should be reported immediately to Visa or MasterCard. These reports should contain explicit details including, transaction dates, times, and other similarities.

When counterfeit card fraud is discovered the accounts should be blocked and reissued. Cardholders should be informed of the need to block their cards and encouraged to review their statements carefully each month for any unauthorized charges.

Counterfeit fraud affecting large groups of accounts should be reported to the United States Secret Service. Issuers should file a Suspicious Activity Reports (SAR) for cases involving large dollar amounts.

Never Received Issue (NRI)

Never received issue fraud occurs when an issuer has sent a card to the cardholder as a new card or a replacement card. The card is intercepted before it reaches the cardholder and is used for unauthorized purchases. Perpetrators are often someone with direct contact to the mail stream for the address to which the card was sent. The perpetrator will steal a single card or a large group of bulk card that will be sold or used by a crime ring. There may be several people involve with the scheme other than the person actually stealing the card.

Never received issue (NRI) fraud can be detected by the cardholder calling the issuer to report the problem or through the detection of excessive activity on the account. Issuers may use pre-and post mailers to alert their cardholders that a new card is coming to them. These documents give the cardholder a warning that they should be looking for a new card to come.

Card activation programs are the most effective tools to stop this type of fraud. Card activation programs may require the cardholder to call from the home telephone number listed on the account before the card will be activated. In most cases, the default is to provide the last four digits of the cardholder's social security number. Issuers should review their card activation reports daily and especially when large card reissues are taking place.

Issuers may want to reduce their exposure to never received issue (NRI) fraud by changing or staggering the reissue cycle for their cards. Issuers with a stable card base may want to have a longer reissue cycle. Issuers with very mobile cardholders may want to reissue more frequently and be sure to verify all addresses before authorizing the cards for production.

Issuers may want to have card delivered to their institution and then given to the cardholder if a high-risk situation has been identified at an address or zip code range where it is convenient for cardholders to come to the institution.

Once a card has been activated, NRI fraud may be detected by the account activity. This detection is usually by a neural network system or by daily authorization monitoring by the issuer. If the fraud is detected after activation of the cards issuers are still encourage to review their card activation reports and issue journal to determine how many cards they may have impacted by the fraud.

Never received issue (NRI) fraud should be reported to the US Postal Inspector's office closest to the address where the card was sent. Issuers should include details on how many cards they had sent to the zip code and the date the cards were ordered and mailed.

The card activation dates and times may help identify a pattern for the fraud. Issuers should note when and where the cards were used and contact the merchants for more information on the suspects using the cards.

Fraudulent Applications

A fraudulent application is produced when a perpetrator uses unauthorized or fictitious personal identifying information to obtain a credit or debit card. Because the perpetrator has no intention to pay for the transactions, excessive activity is very common. In some cases, payments are made to increase the available funds and the payment instruments are found to be fraudulent also.

The best defense for this type of fraud is good internal polices to validate the identity of the person applying for a new card. Third party databases and Issuer's Clearinghouse ICS alerts should be used to help issuers avoid approve of fraudulent applications.

Because the perpetrator is the cardholder, there is greater risk of losses even if a neural network detects the excessive activity. The fraud may not be discovered until the account becomes a collect problem.

Issuers should report fraudulent applications to the US Postal inspection service where the card was sent. If the perpetrator used a "real identity," the fraud should be reported to the US Postal Inspector and local police for the person who has by victimized by the crime. The victim should report the fraud to the credit reporting agencies and the Federal Trade Commission.

The issuer should file a Suspicious Activity Report (SAR) when the fraud meets the federal regulatory guidelines. The issuer may want to file a police report depending on the details of the case. If familiar fraud is involved issuers may be able to have the party pay to avoid the prosecution of a relative.

Account Takeover (ATO)

Account Takeover (ATO) fraud occurs when the account control has been transferred to an unauthorized person as the result of an address change, new card request, adding a user, or pin number change request. In a typical account takeover case, the perpetrator will have the cardholder's address and social security number.

The perpetrator will request that the address be changed to a paid mailbox service or an address that was not authorized by the account owner. Once the address has been changed, the perpetrator will request that a new card and pin number be sent to the new address. When the perpetrator has received the replacement card and new pin, then fraudulent transactions usually occur at an ATM since a new pin. The fraudulent activity will continue on the account until the funds are exhausted. The perpetrator may make fraudulent payments to create new funds on the account.

Account takeover fraud can be avoided by stopping the perpetrator from changing the address or being added to the account. Issuers should have good internal policies to verify the identity of any cardholder requesting an address change. Issuers should investigate any request for a replacement card or new pin within sixty days of an address change. Issuers should require cardholders to update work and home numbers and provide the CVV/CVC 2 code when making an address change via the telephone. When written request are received for address changes the cardholder's signature should be checked against the application signature.

Keeping a list of fraud address will help an issuer to quickly identify this fraud type. Issuers can monitor their account maintenance activity for unlike address changes to major cities, cross-country moves, or address changes to mailboxes.

Cases of account takeover fraud should be reported to the US Postal Inspector in the area where the perpetrator received the card. The address used in the scheme should be documented. The written request should be sent to the agent along with the account detail. The cardholder should be given a new account number and the account should contain a message about the fraud so that the address does not get inadvertently changes again on the new account. All telephone numbers should be verified and updated after the fraud has been discovered.

Card Not Present (CNP)

Card Not Present fraud involves the use of the account information to make purchases with merchants via telephone, mail order, or Internet. These transactions are generally POS entry mode 01. The merchant does not have a physical card present at the time of the transaction The perpetrator may obtain the account number and expiration date for the card in many ways including email schemes, stolen statements, loss or carelessly disposed of receipts. The perpetrator never makes or has a physical card. The transactions are usually excessive and come in suddenly.

Neural networks will generally identify these accounts because of the volume of transactions. Merchants can help reduce this fraud by requesting cardholders to provide their CVV/CVC 2 code for the card or requiring a Verified by Visa or MasterCard secure code enrollment for their customers. Transactions resulting from this type of fraud can be identified by the MCC code and the POS entry mode. Issuers should monitor their daily authorization reports for these types of transactions.

This fraud type should be reported to the merchant to assure that the merchant is aware that the perpetrator is exploiting their system. Merchants are sometimes able to check the purchasers IP address and other information. The FBI or USSS can be notified if large losses exists on the case and several cardholders have been affected by the scheme. Issuers may want to file a Suspicious Activity Report (SAR) depending of the circumstances.

Foreign Fraud

Numerous card issuers nationwide are experiencing international fraudulent activity within their card programs. This fraud pattern is most often linked to information hacking or skimming schemes, and often the accounts affected by these schemes are reported to institutions on compromised account alerts from Visa or MasterCard. Foreign fraud can create some new challenges for your institution, such as:

- How do I explain this to my cardholder when I do not even understand it myself?
- After all, my cardholder is in the United States; what can I do to protect my institution from these foreign losses?

- How do I get law enforcement or regulatory agencies involved and who should it be?

- How do I overcome the difficulties that arise with language and cultural barriers that limit communication between the parties involved?

Foreign Fraud Characteristics

Foreign fraud often results from Phishing, computer hacking, skimming, or Credit Master/Credit Wizard scams. The account information obtained from these scams is then used to commit counterfeit fraud, account takeover fraud or card-not-present fraud over the Internet with foreign merchants.

The foreign fraud we see today has some general characteristics that seem to be a common thread through the majority of the affected accounts. These commonalities may exist because fraud rings or groups, who operate as part of a sophisticated worldwide organization, often commit foreign fraud against many card accounts belonging to cardholders in various locations.

- Domestic card not present transaction "testing" to determine if the account is open. This testing usually involves low dollar Internet authorization attempts that often do not post to the cardholder's account. An issuer may notice an increase in authorization activity from a "test" merchant affecting multiple accounts. The test merchants used change frequently and tend to vary greatly in business affiliation.

- Large foreign authorization activity may appear suddenly, be heavy for a short period of time, taper off as quickly as it began, and then start up in another country. These foreign transactions are frequently purchases at department, electronic, apparel, accessory, and grocery stores, pharmacies, and gas stations.

- Large cash advance transactions. Many perpetrators are seeking cash returns, so cash advances and quasi-cash types of merchants are common.

- Fraudulent activity is currently most common in the following high-risk countries: Australia, Canada, China, France, Great Britain, Hong Kong, Italy, Korea, Mexico, Malaysia, Middle East, Romania, South Africa, Spain, and Turkey.

- The testing and transactions may take place at what appears to be odd times, but this is because often the perpetrator is operating out of a foreign country with a different time zone than the affected area here in the U.S.

- The transactions may only affect one bin, and the account numbers may seem to be used in a sequence. This is common in account s brokered and sold by program, such as, a gold programs or a classic program.

- The same foreign merchants may show up on multiple accounts because of an affiliation with the perpetrator or crime ring.

Researching Foreign Fraud Patterns

When researching the trends associated with a fraud attack look for common threads, similar to the characteristics shown above to establish if this is a. fraud scheme used on various accounts was perpetrated by the same group.

Once a fraud pattern is identified, it is important to check recent data compromise alerts to see if the accounts being used fraudulently appear on an alert or match a pattern described in an alert. If they do, it is important to report this information to the agency listed on the alert.

Use the pattern information that has been uncovered to monitor daily authorization reports within a 30-day period before the fraud attack and current reports to discover any other accounts that may have been affected. This can be done by building a filter around the identified elements and applying that filter to the daily authorization reports to pull accounts that match the set criteria of the filter.

Once you have identified all the accounts affected by a fraud pattern, it is helpful to research these accounts to find a common compromise or purchase point (CPP). Comparing the affected cardholders' past spending histories to see if there is a transaction processed by the same merchant that links the accounts together does this researching process.

In the case of skimmed counterfeit fraud, this is normally the same merchant location. This is because the magnetic stripe on the card was physically captured by some electronic devise at that store. In the case of data compromised counterfeit fraud, the merchant will be the same, but the location of the store can vary.

These compromises occur when a merchant and/or its other branches store valid transaction data and someone hacks into the database storing the information and steels it. If a CPP is uncovered, it may be possible to filter daily authorization reports for the period of compromise to look for other cardholder accounts that were used at this merchant but not yet reflecting a fraud pattern. The CPP and details substantiating these findings should also be reported to Visa and MasterCard so that they may contact the suspected merchant to investigate further.

Protecting Accounts from Foreign Fraud

FIS, Visa, and MasterCard do have options available that can reduce the impact of foreign fraud by restricting authorizations from foreign countries. The decision to implement any authorization restriction is the sole responsibility of the institution. FIS client relations (*or fraud prevention*) should be contacted to obtain guidance and applicable fee information for implementing any of these restrictions.

These restrictions may, in some cases, also restrict cardholders traveling within the country or region and this should be taken into consideration when making the decision. The severity of the situation should be weighed against the negative impact to cardholders. Consider the following:

- The number of accounts impacted by fraud and the total dollar amount.
- The merchant(s) and country(s) of the fraudulent transactions.
- The number of times has the institution been impacted by foreign fraud and can an insurance claim be filed.
- The types of merchants and the dollar amounts of the fraud.
- Whether the merchants that are processing the fraudulent transaction are attempting electronic authorization or in some cases, the merchant is not required to do so because the amounts are below the merchant's authorization limit (merchant floor limit).
- If chargeback rights exist for the fraudulent transactions that have occurred thus far.
- The estimated number of cardholders traveling or living in the country or region where the fraud is occurring.

Authorizations can be restricted for an individual account number or at a level that will protect your bin(s) from potential fraud in a country or region. An institution may contact their FIS client relation representative to request any BIN level restrictions.

The options available at account level are:

- FIS account block- to decline all electronic transactions coming to FIS for the effected account.
- Visa or MasterCard electronic block- to decline all electronic authorization requests coming to these associations for the effected account during stand-in processing.

- MasterCard Warning Notice or Visa Card Recovery Bulletin- to list the account in a paper bulletin that is distributed to the merchants located in the applicable region of listing. This bulletin is to be checked by a merchant when processing an authorization that is under their floor limit. If the account number exists in this bulletin, the issuer has chargeback rights if a transaction is processed.

The options available to protect a BIN are:

- FIS Country Code/Currency Authorization Restriction. This restriction is used to set dollar amount limits allowed for electronic authorizations with a selected country code(s) coming to FIS for authorization. This type of restriction is at FIS corporate identification number level or BIN level and can also be set based on merchant category code or merchant group code, depending on the FIS mainframe system that the accounts reside.

- Visa Risky Table Block – to decline all electronic authorization requests coming to Visa during stand-in processing for a specified BIN(s) from a selected country(s) based on the country code used in the authorization.

- Visa Region BIN Block- to block all electronic and non-electronic authorizations from a chosen region(s) for a specified BIN(s).

- MasterCard does not have a BIN blocking option. They prefer an institution contact the MasterCard Fraud Line or submit a business case describing the fraud situation. MasterCard will review the information and determine how they can help. Contact FIS Fraud Prevention for more information about this option.

Reporting International Fraud to Law Enforcement and Investigative Agencies

An institution's local police department is often not equipped to deal with fraud occurring in other countries but affecting cardholders in the United States. Laws, judicial systems, governments, law enforcement agencies, and cultures can vary from what we are familiar with in the United States. Not knowing where to go or who can help with a foreign fraud situation can cause feelings of confusion, frustration, and hopelessness. Unfortunately, there is not an easy answer for this problem, but there are some options available.

Visa and MasterCard have fraud control offices in foreign countries that provide business connections with international merchants, acquirers, and law enforcement agencies in these countries. An institution may contact USFraudControl@Visa.com or MasterCard at fraudteam@mastercard.com to report international fraud patterns affecting multiple cardholder accounts at their institution.

Individual fraud transactions should be reported through Visa Fraud Reporting or MasterCard SAFE. The data from these reports are analyzed for patterns, connections, and clues to uncover how these schemes are being perpetrated and who may be involved. Common points of purchase uncovered by an institution should also be reported to Visa and MasterCard.

An institution can file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FinCEN) of the Department of Treasury. FinCEN is the Financial Intelligence Unit of the United States and is a member of an international network of 101 countries that have implemented national centers to collect information on suspicious or unusual financial activity from the financial industry, to analyze the data, and to make it available to appropriate national authorities and other Financial Intelligence Units for use in combating terrorist funding and other financial crime. The SAR reports are made available electronically to appropriate law enforcement agencies. Visit www.fincen.gov for additional information.

United States Secret Service is responsible for investigating crimes that involve financial institution fraud, computer and telecommunications fraud, false identification documents, access device fraud, advance fee fraud, electronic funds transfers, and money laundering as it relates to our core violations. To find a Secret Service field office visit www.ustreas.gov/usss/field_offices.shtml

The Federal Bureau of Investigation (FBI) is concerned with transactions that are transacted through wire (Internet) and any terrorist-related transactions. Contact information for FBI field offices is available at www.fbi.gov./contact/fo/fo.htm or an institution can check their local phone book.

Phishing…What is it?

Phishing is a technique used to gain personal information for purposes of identity theft, using fraudulent e-mail messages that appear to come from legitimate sources. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers and passwords, card number and Social Security numbers.

Most phishing e-mails include false statements intended to create the impression that there is an immediate threat or risk to the bank, credit/debit card, or financial account of the person who received the e-mail. Also, people who receive phishing e-mails may not realize that the senders may have used "spamming" (mass e-mailing) techniques to send the e-mail to thousands of people.

Below is an example of a phishing email along with screenshots of a series of events after clicking on the imbedded link:

From: "service@visa.com" <service@visa.com>
Sent: Tuesday, April 17, 2007 7:41 AM
To:
Subject: Your Card is Limited for Online Services!

Dear Visa Cardholder

Continuous Monitoring is an integral part of Visa's multiple layers of security. In addition to other fraud monitoring tools, we can often spot fraud based upon transactions on the card that is outside of cardholders typical purchasing pattern. This allows us to spot fraudulent activity as quickly as possible and acts as an early-warning system to identify fraudulent activity.

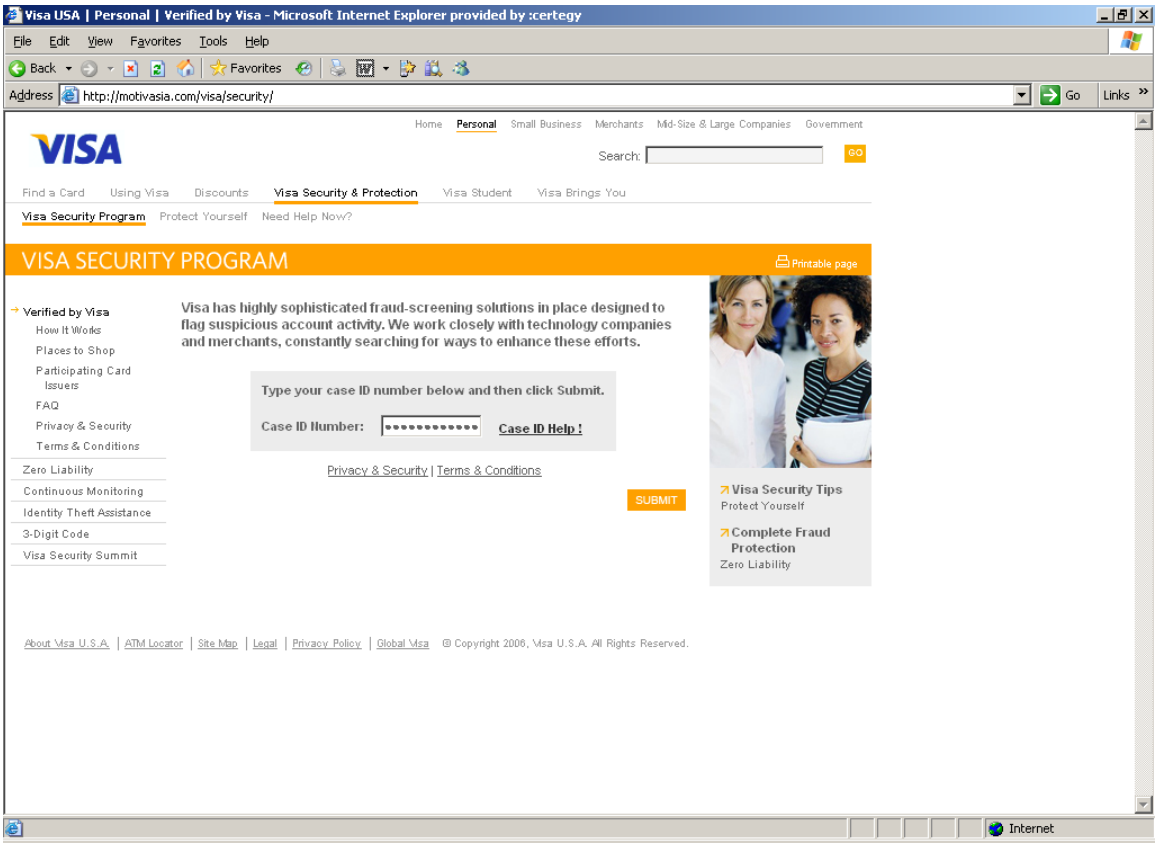
During a recent checkout we detected suspicious activity and your Visa card may have been compromised. Fraudulent activity made it necessary to limit your card for online services, your case ID number for this matter: AT09GP32D506 : Conform to our security requirements and in order to continue online services with your card, we most validate your identity. Please use our link below to proceed.

https://phishingforyourpersonalandfinancialinformation.com

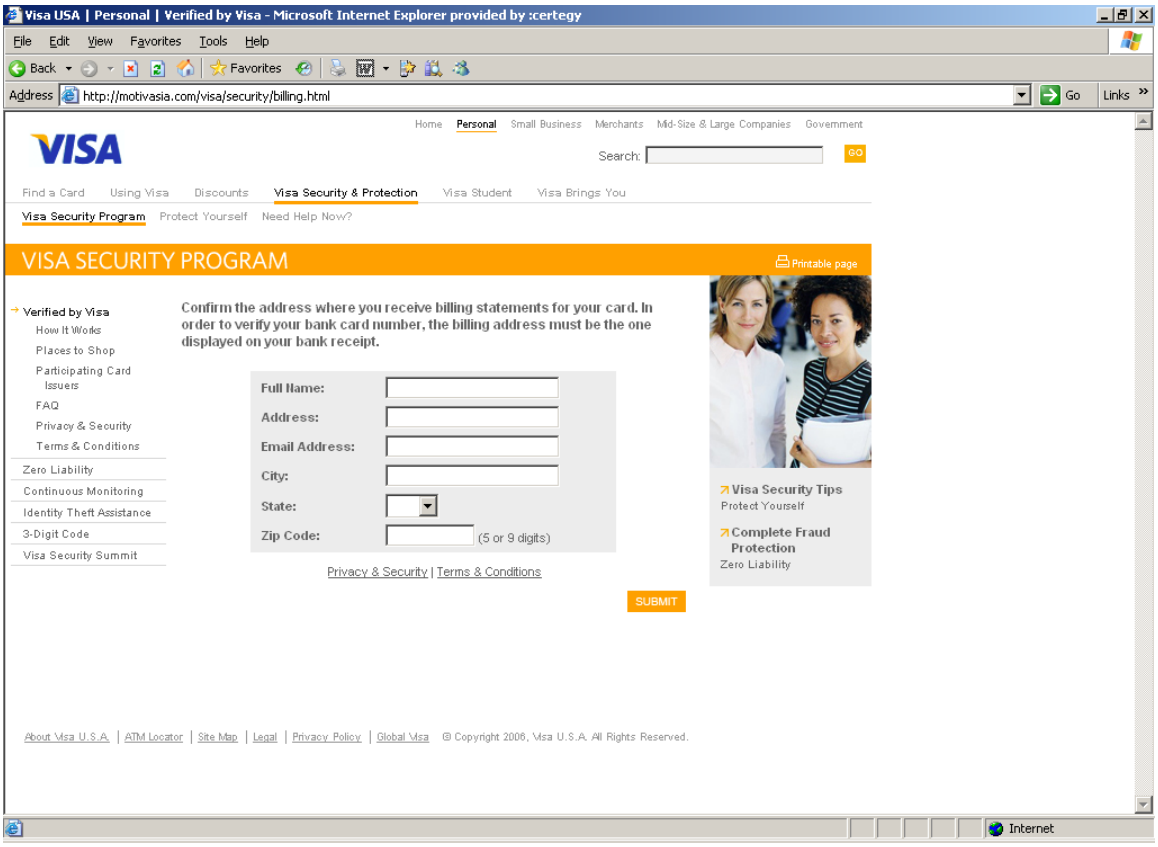
Visa takes online security very seriously so that you can shop safely on the Internet. As part of our commitment to fighting fraud we have the right to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of the terms and conditions for using Visa U.S.A.

Below are screenshots of a spoofed website made to look like Visa's website after the web link was accessed from the phishing email. Let's take a look at the internet address in the URL bar. Does it say it's from Visa.com? That's right it doesn't! This shows you that no matter how authentic the webpage looks you need to verify several tokens before proceeding. (Please see 'Avoiding Phishing Scams" below for more details.)

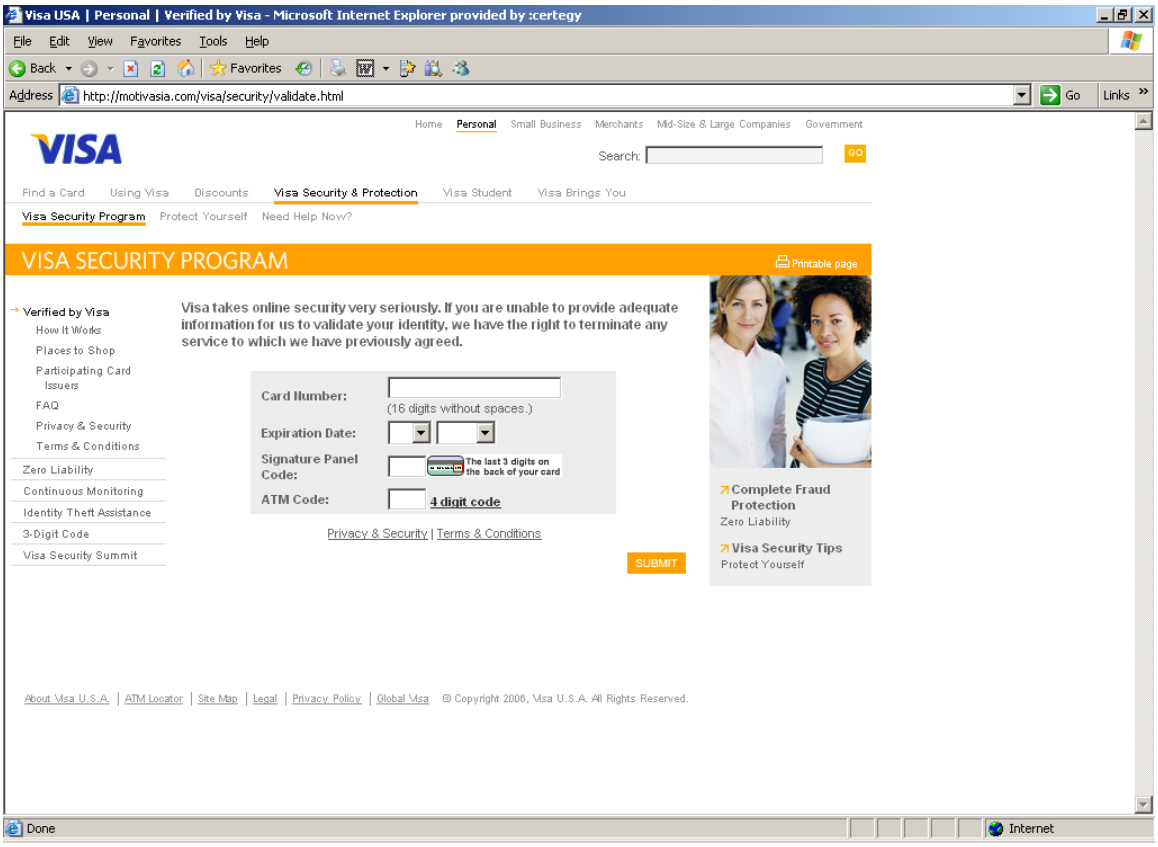
(In the picture below the phisher asks for the case id number that was provided in the phishing email.)



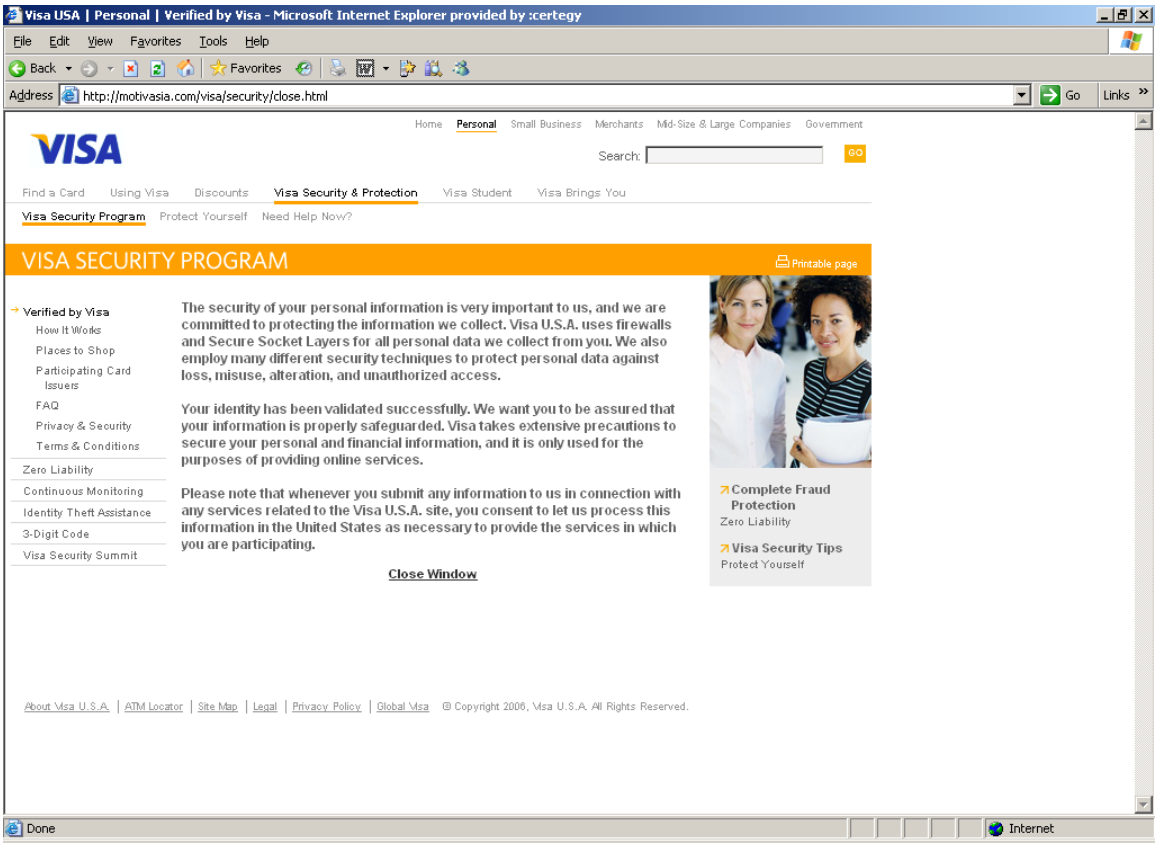
(After the case id has been entered, the next screen shown below populates asking you to confirm your name and address)



(After the personal information has been entered the next screen, pictured below, populates asking for your card information)



(Below is the closing screen after the personal & financial information has been collected.)



So the example shown above is one of many different types of phishing methods that are deployed by the fraudsters. You always want you be aware of several factors: (1). Where did the email originate from? (2). Verify the address in the URL bar. (3). Never provide personal or financial information if you can't verify the source.

Types of Phishing Attacks:

There have been numerous different types of phishing attacks that have been identified. Listed below are some of the more prevalent.

Deceptive Phishing – In this method the phisher uses common social engineering tactics to fool the victim in releasing personal/financial information. Some of the more common tactics used are: "You're account has been blocked", "Congratulations! You've been selected to participate in our Fraud Protection Services". The phisher's goal here is to have the victim act immediately when they open the email.

Malware-based Phishing – Involves running malicious software on user's pc's. Malware can be introduced as an email attachment or as a downloadable file from a website.

Key loggers & Screen loggers – Are several varieties of malware programs that track keyboard input and are able to send the information to the hacker via the internet. These programs can embed themselves into user's browsers that run automatically when the browser is started.

Session Hijacking – is an attack where user's activities are monitored until they sign in to a target account or transaction and establish their login credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

System Reconfiguration Attacks – This attack modifies the settings on the user's PC for malicious purposes.

DNS-Based Phishing AKA "Pharming" – Pharming is the term given to hosts files modifications or Domain Name System (DNS)-based phishing. With a Pharming scheme, hackers tamper with the host files so that requests for website address return a bogus or fake website.

Content-Injection Phishing – Hackers replace part of the content of a legitimate site with false content designed to capture login credentials and/or account number sequence.

Man-in-the-Middle Phishing – In these attacks hackers' position themselves between the user and the legitimate website and collect the data as it's passing from one source to another.

Responding to an Attack

Hopefully, many of you should have some sort of set procedures in place to deal with a phishing attack. Unfortunately, this is one fraud scheme that will continue to evolve as we look into the future. Following are some tips and recommendations when it comes to responding to a phishing attack.

Staff Preparation:

Procedures should be in place for employees to capture and log information to report the incident. These procedures should include:

- Information on the phishing scheme used in the attack – Request and verify the victims email address contacted during the attack.
- Gather all details of the message used in the phishing attack including the imbedded link that was provided in the email. Request the phishing email from the victim. They can either forward it or send as an attachment so that all of the contents are available to you. Also, what type of social engineering method was

used? For example: "Your account has been blocked" or "Your account is past due", or "We noticed some suspicious activity".
- Determine what information was solicited – You want to capture specific details. For example: were they looking for the card number? Expiration date? PIN number? Get as much information as possible.
- Determine what information did the customer provide?

The idea is to collect as much information as you can and to report your findings. (Please see "Reporting the Attack" below.)

Alert Staff and Customers:

- Notify both staff and customers as soon as an attack has been identified.
- Explain what phishing is and what actions can be done when an email message is received.
- Place an article or posting on your website with news of the phishing attempts to inform customers what's occurring in your area.
- Educational materials about phishing can be found at www.antiphishing.org and www.ftc.gov.

How to avoid Phishing scams

While phishing scams continue to increase in terms of velocity and sophistication, consumers should always be aware about what type of personal information is being requested. As a general rule the consumer should never provide personal information to an organization to which they already belong to. Below is a list of recommendations compiled by the Anti-Phishing Working Group (APWG) that one can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal information
  - Phishers use social engineering tactics in hopes of getting the victim to respond as quickly as possible before they realize the scam. This usually includes upsetting or exciting (but false) statements in their emails to get people to react immediately.
  - They typically ask for personal information such as usernames, passwords, credit/debit account numbers, social security numbers, etc.
  - Phishing emails are usually not personalized, but sometimes can be. Valid messages from known trusted sources will usually contain some sort of personalization but we encourage calling and verifying if you are unsure.

- Don't use or click on the links that's been provided in the email, instant message, or chat to get to any web page if you feel that the message might not be authentic or especially if you don't know the sender.
  - Instead, verify with the source via by phone or by visiting their webpage directly by typing in the web address in the browser
- Avoid filling out forms or fields in email messages that ask for personal information.
- Always verify that the website is secure via the web browser when submitting personal sensitive data.
  - Phishers are now able to spoof both the "https://" (that you normally see on secure web server) AND a legitimate looking address in the URL bar. To countermeasure; type in the address of the website instead of clicking on the link provided in the email.

Phishers may also spoof the yellow lock that is normally seen on a secure website shown here.  The lock icon has been considered as an indicator that the website is a secure site. When you double click on the lock icon it should display the security certificate for that site. When the address information does not match between the URL bar and the security certificate, close the browser page immediately.

- If the link provided in the email has been clicked on, verify the address in the URL bar. Be aware of the site that pops up on screen.
- Consider installing a Web browser tool bar to help protect you from known fraudulent websites. These toolbars match where you are going with lists of known phishing Web sites and will alert you.
  - The newer version of Internet Explorer version 7 includes this tool bar as does Firefox version 2
  - There are several tool bars that are free to all internet users and available for download. They are: Netcraft at http://toolbar.netcraft.com/ and EarthLink ScamBlocker at http://www.earthlink.net/earthlinktoolbar
- Regularly log into your online accounts

Make sure that your browser is up to date and security patches installed and applied.

Reporting the Attack

Once you have collected all the information about the phishing attack you should report it immediately to minimize the impact and results. Below are some recommendations to report "phishing" or "spoofed" emails to the following groups:

- reportphishing@antiphishing.org - Submit an email complaint to the link on the left. To do so, create a new email and drop the phishing email from your inbox onto this new email message. Do not forward the email if you can't help it, this approach loses information and requires more manual processing.
- File a complaint with the Internet Crime Complaint Center at www.ic3.gov. This site accepts complaints from either the person who believes they were defrauded or from a third party to the complainant.
- Submit an email complaint to the Federal Trade Commission at spam@uce.gov.
- If Visa's brand is used in the attack, report the incident and forward the email directly to Visa at Phishing@visa.com.
- Also notify the source that is being victimized by the phishing scam. Be sure to forward the email to that source.

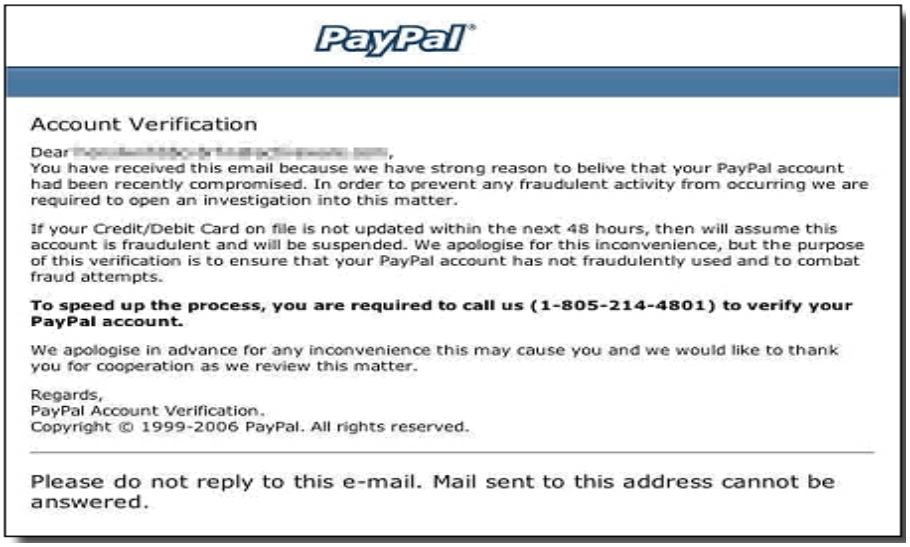
Vishing and SMiShing…What is it?

Vishing also called (Voice Phishing) is the voice counterpart to the phishing scheme. Instead of being directed by an email to a website, the user is asked to make a telephone call. The call triggers a voice response system that asks for the user's personal identifiable information to include: Plastic card number, Expiration date, CVV2/CVC2, and/or PIN number. To date, there have been two methods of this technique that have been identified.

The first method is via "Email blast".

The email blast has the exact same concept of phishing email that includes false statements intended to create the impression that there is an immediate threat or risk to the financial account of the person who receives the email. Instead of Weblink, there is a number provided that instructs the person to call and provide their personal identifiable information.

Example of a vishing email:



PayPal

Account Verification

Dear [redacted],
You have received this email because we have strong reason to belive that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

The second method has been identified as "Cold-Call Vishing".
With this method, the fraudsters use both a war dialer program with a VoIP (Voice over Internet Protocol) technology to cover a specific area code(s). The war dialer is a program that relentlessly dials a large set of phone numbers (cell or landlines) in hopes of finding anything interesting such as voice mail boxes, private branch exchanges (PBX) or even computer modems (dial-up). VoIP is a technology that allows anyone to make a call using a broadband internet connection instead of a regular phone line. VoIP enables the fraudsters to mask or conceal their actual phone number and use a false one to avoid detection. In some cases, the fraudsters have used numbers from local merchants and financial institutions in an effort to gain the trust of the victim.

Example of a War Dialer program:

SMiShing

Smishing is a spin-off version of Vishing. In this instance the victim receives a text message via their cell phone with the implications that there is a threat to their account and request a callback to a number provided in the message. The social engineering tactics used are the same as in the phishing and vishing attacks; the only difference is the delivery method.

Below is an example of a smishing text.
"**(Financial Institution Name) Alert: You're card starting with XXXX has been deactivated. Please contact us at XXX-XXX-XXXX to reactivate your card**".

Responding to an Attack

Following are tips and recommendations when it comes to responding to a vishing/Smishing attack.

Staff Preparation:
Procedures should be in place for employees to capture and log information to report the incident. These procedures should include:

- Information on the phone number used in the attack – Request and verify the victims number that was contacted during the attack.
- Determine what method was the call/message received? Was it a Cell or land line? Was it a voice mail or text message?
- All details of the phone conversation or recorded message – Include the call-out number captured by caller ID or the source of the text message. Also, what type of social engineering method was used? For example: "Your account has been blocked" or "Your account is past due", or more recently "Your account has been breached".
- Determine what information was solicited – You want to capture specific details. For example: were they looking for the card number? Expiration date? PIN number? Get as much information as possible.
- Determine what information did the customer provide?
- Identify the callback number used in the attack.
- Research the callback number and the phone carrier – Fone Finder is a website that helps locate the service provider of the first 7 digits of the area code and phone number used. Their website is as follows: http://www.fonefinder.net/

The idea is to collect as much information as you can and to report your findings. (Please see "Reporting the Attack" below.)

Alert Staff and Customers:

- Notify both staff and customers as soon as a pattern has been identified.
- Explain what Vishing is and what actions can be done when a call or text message is received.
- Place an article or posting on your website with news of the vishing attempts to inform customers what's occurring in your area.
- Educational materials about phone fraud can be found at http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel19.shtm.

"Who's Calling?-Recognize and Report Phone Fraud" PDF available for print and distribution. http://www.ftc.gov/bcp/edu/pubs/consumer/telemarketing/tel19.pdf.

Reporting the Attack

Once all the information about the attack has been obtained you'll want to report it as soon as possible to contain it. Listed below are some steps and procedures in place to help you report the incident.

- Report the incident to local law enforcement – You will need to file a formal report with your local law enforcement agency about the attack.

- Contact the phone carrier's fraud department to get the callback number used in the attack shut down. Usually the phone carriers require a police report file in order to proceed so it's important to have the police report on file.
- Report the incident to the FTC, Federal Trade Commission at http://www.ftc.gov/ or call 1-877-FTC-Help.
- File a report with the Internet Crime Complaint Center at http://www.ic3.gov/default.aspx

Monitoring Daily Reports

FIS provides institutions with detailed reports that focus on various elements of card systems and functionality. It is imperative that you review some key reports to watch for fraud patterns and control abuses on your card portfolio. The most import report to review is the daily authorization report that shows any purchases as well as declines that have been attempted. This report is key in spotting fraud. Other reports to look at are reports that show file maintenance and account status changes. These reports may helps with NRI or ATO fraud. Card activation reports are helpful when NRI fraud has been detected and further investigation is necessary.

For a complete list of report names and characteristics, please refer to Chapter 5 of the Fraud Prevention Guide and the appropriate Reports Guide to understand exact field values on a report.

What to Look for when Monitoring Reports

Manual report monitoring is a way for card issuers to use human intelligence and known fraud trends to help reduce losses and control suspicious spending on their card portfolio.

When monitoring reports you want to focus on the following:

- Excessive activity at a single merchant or on a single account
- Activity outside of your geographic area
- Foreign activity

- Activity during early morning or late night time frames
- Moves to large cities or P.O. boxes
- Credit limit increases or excessive maintenance on an account

Daily Authorization Activity Reports (All Transactions)
This report shows all the transactions on your card portfolio and is the most likely report to indicate fraudulent activity. This report should be reviewed daily and if possible subjected to data mining software to limit its scope since it can contain thousands of transactions per day. Some key characteristics to look for are:

- Large cash advances, not in the cardholder's hometown and/or several in one day
- Unusual times for transactions to occur based on merchant code/type
- Several JS (Jewelry Stores), DS (Department Stores) over $250.00
- Alternating transactions in different cities without adequate travel time between
- Sudden purchasing activity- marked by spending-pattern changes
- Large credit balances or excessive payment activity
- Non-business shopping on business account
- Declined transactions from attempts to the change expiration date
- Repeated transactions for even dollar amounts with OT (Other Retail), DS (Department Store) merchant codes (possible gift certificates)
- Excessive transactions per day or multiple, successive transactions
- Travel/food/gas/car rental/airlines (SIC 3000/5000)
- Hand-keyed or POS 01 during regular hours and DS (Department Stores), JS (Jewelry Stores) merchant codes
- Mismatched data reported like CVV/CVC declines (Code is N7)
- Auth Name Match decline (651)

Any suspicious activity should be verified with the cardholder. Sometimes a review of the statement history may show that the pattern is not unusual for this particular cardholder. An internal policy should be set for when the cards will be blocked and how long the account will remain open if the cardholder cannot be contacted.

Foreign Activity

FIS provides a report of foreign transactions. This report may be helpful when looking for fraudulent activity.

Some focus areas for foreign transactions are:

- Is it reasonable for the cardholder to be involved in foreign travel (based on age/occupation)?
- Several large purchases and/or cash advances
- One merchant charging several accounts
- Transactions occurring at strange times for that country

Card Activation Reports

Card activation reports help when a NRI fraud pattern has developed. These reports may also be reviewed daily looking for potential fraud problems. When reviewing these reports keep these tips in mind:

- Accounts should be activated 10-30 days from issue date
- Failed attempts to activate on several unrelated cards may signal a compromise

Credit Balance Monitoring

Most cardholders only pay what is necessary on their accounts. Excessive payments should be questioned because they give the cardholder more funds to use. Fraudulently used accounts will often show "booster payments" that give the accounts more open to buy after the credit limit has been reached.

When reviewing suspicious payments check the cardholder's past history and watch for:

- Payments exceeding the credit limit with continual charges
- Multiple payments in a cycle period
- Large credit balances resulting from overpaying the account

Address Maintenance

Account takeover fraud generally results from an unauthorized change of address, for this reason quickly checking all address change activity could help you to identify this type of fraud.

Some things to look for on your daily reports and general information screens are:

- Sudden change after long residency
- Change to PO box – Check retail mailbox addresses also
- Change from small town to large risky area (Chicago, IL, NYC, New York, Brooklyn, New York, Houston, TX and suburbs to these cities)

You Discover Suspicious Activity on an Account

When reviewing account for fraud during your usual report monitoring process some accounts will be discovered that exhibit unusual or suspicious activity that may or may not be fraud.

If an account shows a sharp increase in activity:

- First verify the transactions with the cardholder and expect a brief explanation for the excessive spending
- If the charges are not legitimate, verify that the cardholder has not authorized anyone else to use the card and then block the card according to your operating procedures
- If an account displays a known fraudulent address, you will need to verify the address change with your cardholder, place a temporary block on the card and begin researching the address change.
- If you suspect that an account is being used for fraud testing purposes, monitor the account carefully and verify the transactions with the cardholder, if the cardholder cannot be reached place a temporary block on the account until you can verify the transactions.

Handling Special Fraud Related Notifications

Merchant Verifications and Law Enforcement Alerts

You may randomly receive a written notice from a merchant or law enforcement agency requesting your assistance in verifying the authenticity of a transaction. It is important to respond immediately to these requests and to confirm the transactions with your cardholders.

You have received a fax from a merchant or other requesting authority.
Please take the time to thoroughly read and understand the document that came with the alert information. This communication contains important information that will help you decide what steps you should take on your account.

- Contact the cardholder to verify that the transaction is legitimate.
- If the transaction is valid, state this on the faxed document and send back to the merchant, police, or other requesting authority.
- If the transaction is fraudulent:
- Block the card and notify the requesting authority.

Fraud Alert Management Alerts

Fraud Alert Management is a neural network system that uses a combination of fraud trends and cardholder history to identify potentially fraudulent transactions. Fraud Alert Management has a scoring system to decide the level of risk associated with any given transaction and it is this risk score that determines when the transactions will be verified with the cardholder.

It is important to keep your cardholder's telephone number and address current because:

- Fraud Alert Management may need to contact the cardholder to verify the validity of a transaction
- Being able to contact a cardholder could prevent a temporary block on their account if the transaction is the cardholder's.
- If the card is lost or stolen, the cardholder will need to be issued a new card a current valid address will help to avoid possible NRI fraud.

***When personal information is current, Fraud Alert Management procedures are more efficient.

Fraud Alert Management alerts can be a guide to current fraud trends and test merchants. You should review each alert carefully and look for other accounts that may have related fraud but did not score high enough to be contacted by the Fraud Alert Management representatives.

Keep all Fraud Alert Management alerts for future reference, some fraud patterns take several months to create a pattern that can be recognized.

Please refer to the Fraud Alert Management Operating Guide located on the E-Library.

Account Compromises –Visa Compromised Account Management System (CAMS) and MasterCard Alerts

Visa CAMS and MasterCard Alerts are programs to inform card issuers of the circumstances relating to a known card account compromise and to provide a list of account numbers that have been identified as "at risk" due to such exposure. These alerts are created when Visa and MasterCard have been alerted of a compromise that may include one or more of the following events:

- Potential database compromise due to computer intrusion (hacking),
- Skimming operation
- Account numbers posted on the Internet
- Account information found during an investigation or arrest
- An account range displaying unusual testing type activity found during authorization monitoring.
- Phishing and spoofing schemes
- Stolen equipment or documents containing card account information

Establishing policies and/or guidelines to address alerts can take the guesswork out of deciding the best action to take each time a new notice is sent out. Alerts should be addressed immediately when they are received. Consider the following smart ways to deal with account compromises.

Evaluate the alert.
Determine if the compromise was high-risk or low-risk by examining the details of the compromise provided in the alert notification. High-risk compromises include situations in which the magnetic stripe information has been obtained, high fraudulent activity levels have been reported, or other sensitive personal cardholder information was also compromised. Moderate to low-risk compromises include situations in which only the account number or partial data was exposed, no known fraud has been reported on the accounts affected by the compromise, the "leak" has been repaired, or the account data is very old.

Evaluate your situation. (Use your Inquiry Screens)
Find out how many of the compromised accounts are still active. If there are some non-active accounts, determine how many of them have been closed due to fraud because this may imply that the perpetrators will be using other accounts soon.

If you have closed accounts that were involved in fraud, you should look at the statement history to see if the fraud pattern on the closed accounts matches up with the circumstances or fraud pattern described in the alerts message. For example, if the notice describes a fraud pattern of full magnetic stripe counterfeit taking place, you should determine if your fraud patterns are similar. (These will be your POS 90 transactions on your Daily Authorization Report. The BC 583-01 -CP211004 or PD238.).

If the fraud alert describes a compromise involving only account numbers and expiration dates, you may be looking for card-not-present fraud patterns. (These will be your POS 01 transactions on your Daily Authorization Report. The BC 583-01 -CP211004 or PD238.

If you detect similar fraud patterns, you may want to consider blocking and reissuing cards for the affected "active" accounts using these best practices as a guide. Fraud patterns matching the kind of data elements compromised are often telltale signs that someone has already obtained some of your accounts and has used them. So, the other accounts may be exposed as well.

If you have not seen any signs of fraud that you believe could be linked to the reported account compromise incident, apply the following ideas accordingly. You need to keep in mind that it is often difficult to determine if the hacker was able to retrieve all of the exposed account numbers, including those from your institution.

Narrow down the high-risk possibilities.
For incidents involving the compromise of full track data, (This is all the data in the magnetic stripe which includes CVV or CVC) find out if any of the accounts were reissued after the compromise date. If so, you may not need to consider these accounts as "high-risk", since they would have been

reissued with a different Card Verification Value (CVV) or Card Verification Code (CVC) and expiration date.

Check for upcoming expirations.
Of the affected accounts, determine how many of them will be expiring in the next 30 to 180 days. Consider moving up the reissue on those accounts.

Do a fraud exposure reality check.
Take into consideration the number of cards affected, daily spending limits on cards, and the likelihood that fraud may occur. Also, assess the likelihood that the fraud will take place in the card-not-present environment, which may give you charge back rights for fraudulent transactions. Know your normal fraud rates. How do these accounts measure against your normal fraud rates? Are they higher or lower? Higher than normal fraud rates may require you to examine all options including cost and reissue.

Know your insurance rights and liabilities.
If you are a credit union and have counterfeit fraud insurance coverage, you may need to review your coverage with your carrier and discuss the impact of not blocking and reissuing new cards.

Stay one step ahead of fraud exposure.
Examine the possibility of you or your processor monitoring low risk compromised accounts using a fraud management system. Also, consider blocking and reissuing accounts that you have identified as high-risk.

Pay attention to follow-up notices.
Alerts are often released before the investigation is completed. Additional findings may be distributed via a subsequent alert. Visa and MasterCard continue to monitor compromised accounts through their internal systems and will notify issuers if any unusual activity or patterns are detected. This does not mean that you should discontinue monitoring these accounts.

Keep Visa and MasterCard in the loop.
Always let these associations know if you have experienced fraud that you would consider related to a compromise incident, or if you begin experiencing fraud on any of the compromised accounts. Visa Fraud Control's telephone number is 650-432-2978 and email address USFraudControl@Visa.com or MasterCard at fraudteam@mastercard.com. Some alerts request that issuers report specific information regarding the compromise to another investigative party. It is important for the success of the investigation to provide the requested information.

Think before you list.
If you do block and reissue compromised accounts, carefully assess the cost/benefit of listing these accounts on the Visa Card Recovery Bulletin or MasterCard Warning Notice. Given the "per card" costs involved to list accounts with foreign fraudulent activity on the Recovery Bulletin or Warning notice, this service should be used prudently. You, of course, want to minimize the risk of continued losses, but in the end is it worth the expense of doing so?

Archive your Alerts.
At times, a past alert must be referenced when filing a compliance claim for magnetic stripe compromised fraud transactions. MasterCard periodically offers the opportunity to file a Claims Reimbursement request and the original alert information must be provided when doing so.

An account that was on an alert but an issuer had chosen not to block may later experience fraud and it is helpful to have the details of the alert available to assist in your fraud prevention efforts.

For institutions that do not download their alerts. Instead, FIS is performing this function, E-Archiving is available. The cost of this service is $50.00 a month for one CD and $25.00 for each additional. For those institutions that download their alerts, Visa retains alert archive data for 45 days only, and MasterCard retains a complete archive.

Resources

Included in this best practice guide is a list of websites that prove to be resourceful and can help your institution learn about or manage different aspects of fraud. The following section provides resources to aid those who are researching information on fraud topics, current fraud trends, organizations, and government agencies.

Anti-Phishing Working Group (APWG) – www.antiphishing.org.
The anti-phishing work group is focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The website provides a forum to discuss phishing issues and share information while offering best practices to eliminate the problem.

Credit Bureaus
Financial Institutions can contact the three main credit bureaus to investigate the credit history of current or prospective customers. Institutions and cardholders can also contact the credit bureaus if the following fraud types can be identified such as: Fraudulent Applications, Identity Theft, or Telemarketing Schemes. Here is a list of the three main Credit Bureaus:

- **Equifax Credit Information** – www.equifax.com. Phone number is (800) 997-2493. Fraud Line (800) 525-6285.
- **Experian** – www.experian.com. Phone number is (888) 397-3742.
- **Trans Union** – www.transunion.com. Phone number is (800) 888-4213.

Federal Bureau of Investigations (FBI) – www.FBI.gov.
Phone number is (202) 324-3000.Financial Institutions can contact the FBI to obtain information about or report large-scale crimes. These crimes can include: Computer Hacking, Nigerian Schemes a.k.a. (Advance Fee Scheme), Counterfeit, & Terrorist Concerns.

Federal Trade Commission (FTC) – www.ftc.gov.
Phone number is (877) 382-4357. The FTC developed and maintains the websites of the Consumer Sentinel and the Identity Theft Data Clearinghouse (ITDC). Financial Institutions can get the facts about consumer fraud such as: Internet cons, Fraudulent prize promotions, Work at home schemes, Telemarketing scams, and **Identity theft**. Institutions can also learn about the trends of complaints that consumers file, especially, **Identity Theft**.

International Association of Financial Crime Investigators (IAFCI) – www.iaci.org.
This website offers information about financial fraud, fraud investigation, and fraud prevention methods from various agencies in both the financial payment industry and law enforcement from around the world.

MasterCard International – www.mastercardintl.com.
Phone Number is (800) 307-7309 and / or (914) 249-2000. Like Visa, MasterCard has an abundance of information in regards to their product and offers risk-solution information to help combat the elements of fraud.

United States Department of Justice – www.usdoj.gov.
Phone number is (202) 353-1555. The Criminal Division / Fraud Section of the Department of Justice plays a unique role in the fight against sophisticated economic crime. Although, It's main focus is combating white-collar crime, there is an abundance of information in regards to Internet fraud, Identity theft and Identity fraud, as well as special reports on "Phishing".

United States Postal Inspectors (USPIS) – www.usps.gov.
Phone number is (202) 268-4396. Financial Institutions can contact the U.S.P.I.S. to obtain information about high-risk mailing areas identified by Zip code and to report NRI Fraud. Identifying these areas can help institutions reduce their exposure to Not-Received Issues also known as NRI Fraud.

United States Secret Service (USSS) – www.secretservice.gov.
Phone Number is (202) 406-5708. Both the Secret Service and the FBI have investigative responsibilities that include: Financial Institution fraud, Computer and Telecommunications fraud, Access Device fraud, & Money Laundering. Financial Institutions can also contact the Secret Service to report large-scale crimes.

Visa International – www.visa.com.
Phone Number is (650) 432-2978. This website offers a wide range of information pertaining to the Visa Product. An informative section to take note of, Is the Operations and Risk Management section. Information such as: Basics of Fraud Control, Cardholder Information Security Program (CISP), & Verified By Visa are helpful.

FIS Fraud Prevention and Investigative Services
The FIS Fraud Prevention team was developed to assist financial institutions in understanding, preventing, and researching fraud loss affiliated with their card programs. Through the utilization of the Fraud Hotline service, the team is available to provide expert advice on topics concerning card fraud trends, authorization parameters, report monitoring, and case data development.

The Fraud Prevention Department guides clients through industry recommended best practices for fraud investigation and reporting. The team combines their expertise with current technology to help financial institutions prevent fraud and reduce global economic crimes. The department also provides predetermined contractual investigative services to FIS financial institutions that may not have the resources available to fully address high-dollar fraud cases.

Often the department employs the assistance of federal law enforcement agencies, such as the United States Secret Service (USSS), United States Postal Inspection Service (USPIS), and the Federal Bureau of Investigations (FBI). The team may call upon and utilize resources from Visa, MasterCard, Financial Institutions, other third party processors, and industry associations, like the International Association of Financial Crimes Investigators (IAFCI).

In addition, the Fraud Prevention team designs and delivers classroom, web-based, and computer-based training classes covering a myriad of fraud topics in an effort to ensure our financial institutions have the knowledge they need to prevent and detect fraud.

Fraud Prevention Expertise

Our Fraud Prevention team is especially knowledgeable about various techniques used to identify, stop, and prevent fraud losses in light of the current fraud trends within the credit / debit card industry worldwide. The team assists FIS clients by providing a well-developed, customized, strategic plan that is appropriately designed based on the details of the fraud situation and the operational restraints of the financial institution.

The FIS Fraud Prevention team has a proven track record of organized fraud case management, having provided many financial institutions with trusted expert investigative assistance for both internal and external fraud cases.

Our goal is to provide a quality service to address your fraud management concerns. If you suspect fraudulent activity on your credit or debit program, or if you would like to incorporate a proactive fraud management plan *before* fraud hits, call the FIS Fraud Prevention team.