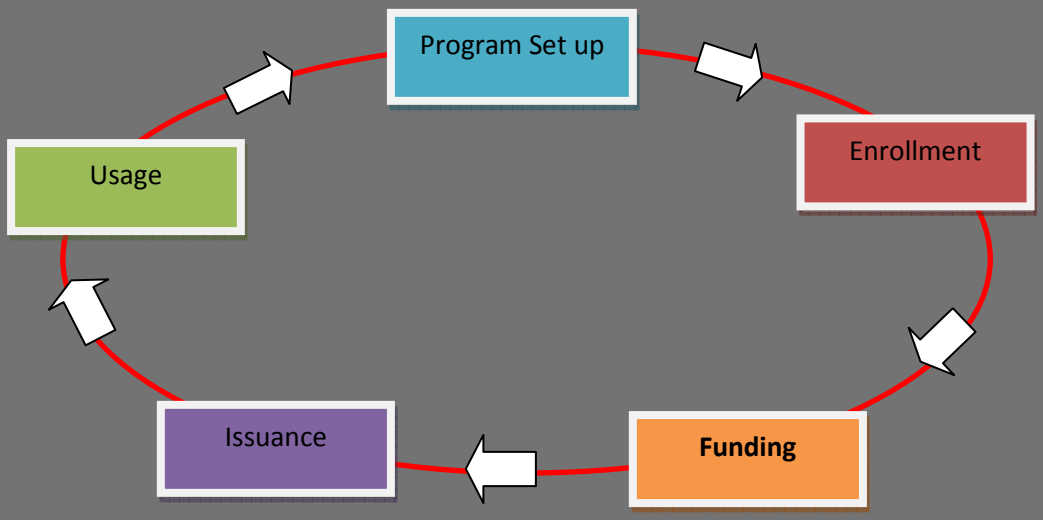
2011

Fraud Mitigation

Prepaid Card

Leveraging our processing relationships to prevent fraud throughout the prepaid cycle



CanaCash Financial Services Ltd.
1/1/2011

Table of Contents

Introduction

Prepaid issuance and program management has undergone tremendous expansion, with the largest programs reaching multi-millions of cards issued. This expansion also provides for a potentially higher level of risk exposure. Prepaid issuers and program managers must pay an increasing amount of attention to fraud issues, anticipating the next moves of fraudsters and managing fraud within the prepaid arena. Implementing the strategic initiatives and employing the tactical tools to prevent fraud on prepaid accounts must be the driving goal. Addressing fraud concerns proactively before pre-paid fraud has the opportunity to blossom will result in greater trust among cardholders, greater transactional volume, and a more smoothly run prepaid program.

Issuers and program managers are not alone in this journey to mitigate and contain fraud. The prepaid processor can provide insight and assistance in coordinating, managing and organizing a fraud mitigation strategy. This manual will examine the potential sources and some of the most common methods of perpetrating prepaid fraud. We will also examine how prepaid industry participants including prepaid issuers, program managers and processors fight prepaid fraud. And finally we will provide insight into the future of prepaid fraud mitigation, how pre-paid processors are providing additional services and integration into the fraud mitigation process to create a more symbolic relationship with program managers and issuers.

Falcon Risk Mitigation

Prevention through Detection

Falcon Risk Mitigation

Fraud Detection

Our transactional fraud detection program is focused on allowing us to observe unusual patterns of purchase behavior in retail transactions and to take positive action to curtail the fraudulent activity. We offer an optional service for fraud detection that utilizes neural-based detection systems, such as Falcon to detect activity that may indicate fraudulent activity.

The Falcon system, powered by Fair Isaac, Inc, is used by FIS Prepaid to detect and ultimate prevent fraudulent transactions on our clients' stored value products. Falcon is a neural network –based, predictive software application that examines transactional, cardholder and merchant data to detect a wide range of payment card fraud. Falcon reviews each authorized transaction, and based on historical behavior, provides a score from 0 to 999. This score represents the probability of the individual transaction being related to fraudulent activity. The higher the score, the higher the chance it is a fraudulent transaction. Transactions are scored in near real-time, generally within 1 to 2 seconds after the authorization occurs. Our detection system uses the Falcon score to take the appropriate action for accounts where transactions scores have exceeded program defined levels. One of the primary control methods FIS Prepaid in place is the ability to automatically change the status of an account (Potential Fraud or Suspended) based on client defined criteria in Falcon action rules. Auto-statusing of an account is usually used in conjunction with auto e-mail notification to the buyer or cardholder post authorization.

eFalcon

The eFalcon system is used by FIS Prepaid Solutions Systems to detect and ultimately prevent fraudulent funding on to our clients' stored value products. eFalcon is a neural network tool that examines the load activity, respectively looking for patterns that indicate fraud is occurring (i.e. commercial billing address). The e-Falcon tool uses historical data to create behavioral models. Value loads are scored from this model, receiving a higher score when the probability of fraud increases. Scores will range from 100 (lower risk) to 999 (higher risk).

Enrollment Validation

One of the areas of potential risk exposure with a card program is the consumer enrollment data. In many Payroll Program circumstances the employer is directly involved in the enrollment process and can perform validation of the enrollee and their data. However, there are other means of enrollment, particularly self-enrollment, where the employer is not directly involved and therefore is not performing validation.

FIS Prepaid Solutions offers a risk management service called the Enrollment Data Verification Service. This service captures enrollment data and sends it out to a verification service called RiskWise. RiskWise provides a verification score, which a program can used to derive an approval decision regarding opening the account and mailing a card.

During the enrollment process, key fields in the enrollment application – name, address, telephone number, social insurance number and date of birth – are captured, formatted and then sent to RiskWise for verification. RiskWise uses a variety of databases to verify the data. A score (with potential problem information, if indicated) is then returned to FIS and that data/decision can be acted on at the end of the enrollment process. Clients will provide their own criteria for scoring and decision

Background

Our corporate fraud policy is established to facilitate the development of controls that will be in the detection and prevention of fraud against the company. It is the intent of our company to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.

Scope

This policy applies to any irregularity or suspected irregularities involving employees as well as shareholders consultants and vendors contractors outside agencies doing business with employees of such agencies and any other party with a business relationship with our company. Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position title, or relationship to the company.

Policy

Management is responsible for the detection and prevention of fraud, misappropriations and other irregularities. Fraud is defined as the intentional false representation or concealment of a material fact for the purposes of inducing another to act upon it to his or her injury. Each member of the management team will be informed of all types of improprieties that might occur within his or her area of responsibility and be alert for any indication of an irregularity. Any irregularity that is detected or suspected must be reported immediately to the shareholders, partners, who coordinates all investigations with the legal department and other affected areas both internally and external.

Actions Constituting Fraud

The terms of the misrepresentation and misappropriation and other fiscal irregulars referred to, but are not limited to;

- Any dishonest or fraudulent act
- misappropriation of funds, securities, supplies or other assets
- impropriety in the handling or reporting of money or financial transactions
- profiteering as result of insider knowledge of company activities
- disclosing confidential and proprietary information to outside parties
- disclosing to other persons securities activities engaged in or contemplated by the company
- accepting or seeking anything material value from contractors, vendors, or other persons providing services materials to the company. Exceptions: gifts less than $25 in value
- destruction, removal, or inappropriate use of records, furniture fixtures and equipment and or
- any similar or related irregularity

Other Irregularities

Irregularities concerning an employee's moral, ethical, or behavioral conduct should be reported to the partner management. If there is any questions as to whether an action constitutes fraud, contact the shareholders (partners) for guidance.

Investigative Responsibilities

The partners have the primary responsibility for the investigation of all suspected fraudulent acts as defined in this policy. If the investigation substantiates that fraudulent activities have occurred; the partners will issue reports to appropriate the designated personnel for further action.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and or regulatory agencies for independent investigation will be made by the partners with legal counsel and senior management, as will final decisions on disposition of the case.

Fraud Overview

There are a variety of fraud types that are impacting prepaid programs. Most are centered either on the fraudulent use of funding sources to load prepaid accounts, or the manipulation of the transaction processing system to place more funding on the card and actually should be there. In either instance, the prepaid program is exposed to financial losses and bears the liability for such losses. The fraud occurring on prepaid accounts generally capitalizes on several points of compromise.

- Prepaid account enrollment
- issuance and activation of the cards
- loading or funding the cards, and
- purchase transactions or cash access

Prepaid program risk managers are building on the risk mitigation foundation that prepaid processors and other partners are providing. But they are also taking that foundation and leveraging it for a more aggressive stand against fraud. The overriding goal of risk managers on the cutting edge is to move from fraud detection to actual fraud prevention.

To minimize exposure to fraud losses, it is integral for issuers and program managers to move to prevention and dealing with fraud. Established card issuing financial institutions may have figured this out, but those like us who are just entering the issuing arena could benefit by outsourcing some of the fraud prevention programs to prepaid processors and other partners. Processors that have the experience and have made the investment in an evolving fraud management offering can bring new prepaid programs into function quickly and safely, minimizing fraud exposure. The processors that will serve the prepaid community best in the coming years will integrate world-class prevention capabilities that provide effective risk mitigation and also defray the cost to program managers of having such programs in place.

Two overriding principles rule the fraud prevention mindset;

- Don't let this card get in fraudsters hands, and
- make sure it's a legitimate funding source for cards loads

Prepaid program managers seeking to move to the prevention mindset for fraud will consistently come back to these two principles. The centerpiece of any viable prevention oriented fraud mitigation program will be based on getting as close as possible to making sure neither of the above happen. Preparation is the key, and through the combined efforts in diligence of prepaid processors, issuers, and program managers, growth and prepaid fraud can be pro-actively avoided.

Prepaid program risk managers can utilize the prepaid processor to a large extent for fraud mitigation efforts. The processor provides in-depth data on transactions and other activity on each account, giving the program risk manager valuable insight and leverage in detecting fraud. The relationship and inner action is important in the risk management foundation that processors have built in the prepaid arena can provide the foundation needed in managing prepaid fraud, including;

- Identification of the card holder and prepaid card purchases
- detection of patterns or fraudulent transactions on prepaid accounts

But this also extends to other risk factors and financial activities, including changes to address, changes to source account information, changing e-mail addresses and other personal information, and analyzing the velocity with which this is done by cardholders and card purchasers. This information can be used effectively to create a more complete risk profile for prepaid card products.

Prepaid risk managers are seeking to be more proactive in this antifraud effort, not only identifying trends early enough to mitigate the losses, but taking action on identity and behavior to eliminate many instances of fraud. The processor relationship, the tools, and intelligent data and knowledge sharing the processor can provide to issuers and program managers can be quite important and useful to this effort.

In many instances, the prepaid processor has been integral in providing not only a framework for combating fraud, but also in setting up the partner relationships that allow for additional checks. This foundation and indeed the foundation for overall fraud management is built in combination with the compliance programs the processor puts into place and other regulatory compliance inherent to all prepaid programs in the tools the processor makes available for such compliance programs.

Processors also provide data on card activity, a direct feed, online tools and or specific reports in the way that prepaid program risk managers needed and can most effectively use it. The processor view is that much broader than that of individual program managers and can greatly assist in discovering and even thwarting additional cases of fraud. The bottom line, however, is that the solutions in use today are principally reactive. The additional effort and working the fraud cases can be a challenging, labor-intensive task. Getting to fraud prevention from fraud detection and resolution therefore often depends on the processor, issuer and program manager working in conjunction. Additionally, successful processors will continue to invest in fraud management tools. Fraud management is not a static undertaking. The processor that maintains up to date processes and antifraud tools represents a more valuable partner for the issuer and program manager.

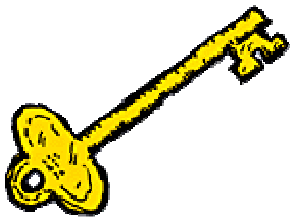
Prepaid risk and fraud managers also see the value of involving the cardholder and fraud mitigation. This takes the form of actionable alerts that can be sent to the cardholder during the course of a questionable transaction. But this can also take the form of simple transaction or balance alerts that keep the cardholder better aware of card usage and may alert them to an account compromise. It is the cardholder who can best recognize legitimate account activity and stop fraudulent transactions in their tracks. Involving the customer and fraud mitigation and working with the processor that more easily enables this involvement is one successful means of moving from fraud detection to fraud prevention.

A major step in moving from fraud detection to actual prevention is to align processor capabilities with program manager needs. Through the processor and program manager desire the same success for the prepaid program, program managers see themselves as the last line of defense, and as bearing most of the risk of losses. They key in the relationship is defining the needs and capabilities that complement the capabilities of the program manager. This may be more customized for more establish prepaid programs with robust and developed risk management teams and plans. While new programs managers may be looking for more of a turnkey processing solution that extends into program and risk management they may find that they must rely on outsourced support or expertise.

Comprehensive or real-time data from a processing partner and the insights that can be gleaned from a broader base of data may, in many cases, exceed the act which individual companies can achieve on their own. Fraud mitigation is also inherently enhanced by additional sources of data and information. Effectiveness is gained through the broader perspective the processor can bring and through the ability to share best practices across the portfolio of prepaid programs.

The processor can represent an additional line of defense and fraud mitigation, but issuers and program managers will need to integrate the processor into their own fraud mitigation process, even if it may require dedicated and extended efforts. The rewards from such efforts could prove to be tremendous.

DETECTION TO PREVENTION THIS THE



Working with Your Processor

Though the prepaid industry has not experienced a major uptick in fraud, diligence is necessary to pro actively avoid such a situation. Processors who can assist and engage in the fraud mitigation process as prepaid transaction volume grows will be more valuable to issuers and program managers. As more money is placed on prepaid cards, the prepaid world becomes a more enticing target. Simultaneously the types of prepaid cards in the marketplace are designed for more transaction velocity and greater length of use. A payroll or general purpose reloadable card for example is used for more transaction and has more funds loaded onto it on average over its lifetime than a gift card.

The opportunity not only to steal the card information, but also to benefit from the theft is that much greater for the fraudster. The ability to both scale transaction volume and also mitigate fraud is of vital importance for the selection of a pre-paid processor. As importantly, fraud reduces profits. With large players such as Wal-Mart cutting fees for prepaid cards, downward pressure on profit margin seems inevitable and makes effective fraud management that much more imperative.

- Prepaid program managers and issuers must work with their processors to address specific points of vulnerability in the prepaid account process. The key aspects of fraud mitigation center around keeping cards out of the hands of fraudsters and ensuring that the funds loaded onto the card are good funds, and not subject to charge backs and coming from legitimate sources.

Resolution and Detection

Prepaid accounts, like debit cards, have available funds on them that can be taken over and used by fraudsters, thus depleting the value. However, account fraud affects prepaid in ways that are different from debit and credit cards, for example, existing credit cards, debit cards or non-card accounts, can be used fraudulently to purchase and load funds on prepaid cards.

It is therefore very important that you defective prepaid risk mitigation and monitoring looks at the purchase of the card and the fund loading transaction as among the most vulnerable pieces of the prepaid process. Viable risk management programs pay particular attention to these transaction types. The prepaid processor can provide more effective reporting and another layer of analysis in each of these situations.

It is integral for issuers and program managers to move to prevention in dealing with fraud. Establish prepaid issuing financial institutions with dedicated risk departments may have figured this out, but those who are just entering into the prepaid arena could benefit by outsourcing some of the fraud prevention programs to prepaid processors and other partners. The processors that will serve the prepaid community best in the coming years will integrate world-class prevention capabilities that provide effective risk mitigation and also defray the cost to program managers of having such programs in place.

Resolution: after the fact customer relationship Management

Resolution in making the customer whole again after fraud occurs is important in maintaining the customer relationship, but doesn't pro actively address the root of the fraud. It is the most downstream aspect of fraud management. Examples of resolution policies include zero liability protections for cardholders, dispute processing, CSR teams dedicated to resolving fraud issues, fraud analysts reviewing exception reports, assisting with law enforcement interaction, among other reactive policies. Financial institutions have historically dedicated a decent proportion of overall fraud mitigation efforts to transactional fraud resolution for their credit and debit portfolios because they recognize the importance of ensuring that the damage doesn't adversely affect the greater customer relationship. Prepaid products may have fewer transactions but they are also intended to strive for extending cardholder relationships. This makes fraud resolution policies equally important in the prepaid arena. Historically, most prepaid fraud resolution efforts fell within the prepaid issuer and program manager. There is a current trend to more actively to involve prepaid processors as well as other third parties in combating fraud and thus creating a vested interest in maintaining the ongoing cardholder relationship.

Resolution and Detection

Moving upstream from after-the-fact resolution is detection of fraudulent activity on prepaid accounts. The majority of prepaid fraud mitigation efforts and the prime area of coordination amongst processors, issuers, and program managers is the detection of potential fraudulent activity. Statistics consistently show that early detection of fraud leads to lower overall losses for all types of existing card fraud. Giving fraudsters less time with stolen account information mitigates fraud. Statistics show that the average out-of-pocket costs paid by consumer victims of identity fraud by the time it took to detect the fraud both the actual numbers and statistics are lower. The average consumer out-of-pocket cost rises as the detection time for the fraud event is extended. Assistance with early detection can affect the overall losses for cardholders, prepaid issuers and program managers.

Detecting fraudulent loads using compromised data or credit cards early is very important as these cards are historically used to either load multiple cards or to make recurring loads until the fraud is detected. The issuer or program manager must partner with the process to scan the portfolio for other instances where the compromise funding account may be being used. A key control is to establish credit checks to ensure that the funding account information entered, such as names and addresses matches the information that is included in the profile of the person who is funding the account. Many times these two profiles are different because the fraudster must use the legitimate address of the stolen card to pass address validation. When fraudulent funding sources are identified the numbers should be placed on watch lists so that any future use of the funding account number is flagged and reviewed. Velocity monitoring on the number of times and the dollar value of funding by a specific funding source as well as the number of funding account additions or changes relating to a profile are also important controls to implement with the processor.

Doing it Better

In defining risk mitigation strategies and specific tactics, prepaid issuers and program manager should leverage processor expertise, industry knowledge, partners and technology solutions to develop an overall framework. What are the basic pieces of fraud management that processors can help manage?

The data of the individual issuers and program managers have is not typically as comprehensive or real time as that of their processing partner. And the insights that can be gleaned from a broader base of data may, in many cases, exceed data which individual stakeholders can achieve on their own. Fraud mitigation is inherently enhanced by additional sources of data and information.

From the overall risk mitigation strategy to specific tactics, the prepaid processor can bring expertise and industry knowledge, partners and technology solutions, as well as an overall framework by which to attack fraud. We'll now look at the approach to fraud management and its various forms and how processors, issuers, and program managers can most effectively work together on that approach. Prepaid processors can provide assistance to issuer and prepaid program managers with broad mitigation in a broad sense. This is often an area for which program managers and risk managers within prepaid programs are reluctant to cede any form of control to the processor or to any other partner. The historical perspective has been that the program manager is not only closest to the front lines and therefore is in the best position to fight fraud but also that the processor and other partners have little vested interest in actually reducing fraud within the prepaid program. Yet the processor can provide individual program managers with insights that might otherwise be foregone. Effectiveness is gained through the broader perspective the processor can bring, and through the ability to share best practices across the portfolio of prepaid programs.

A higher degree of confidence and integration with the processor can result in more honed and effective risk mitigation in specific prepaid programs. The processor that will try moving forward are those that can proactively provide fraud and risk mitigation tools to those program managers that may not have the innate ability, the experience, or that track record to do so themselves. The productive relationship between prepaid issuer and processor is one that takes full advantage of all capabilities the processor has, moving well beyond simple nuts and bolts transactional processing to an in-depth interaction particularly with regards to risk management. This is seen in the development of risk mitigation strategy and the flow of data from processor to issuer and provide insight into what transactions should be red flagged as potential fraud and also in the tactics and tools that can be applied to mitigate prepaid fraud.

Core Competency; Where to Look

Many established prepaid issuers and program managers work from the position that actual fraud management is done within their own arenas. These programs have the internal knowledge to identify productivity and trends and then stop the fraud in its tracks. For these issuers, it is generally a difficult proposition to get from a reactive or even semi-reactive stance to a proactive stance in fraud mitigation. There is a reluctance to cede control to third parties such as prepaid processors in managing risk, especially when the liability for such risk remains with the issuer. Several prepaid program risk managers describe this internal risk management process as incredibly labor-intensive, but in the end incredibly valuable.

Visa debit processing service has been able to reduce monthly fraud losses from load fraud as much a 65% by implementing proactive preventative measures to stop the fraudulent enrollment contact the fraudulent load before money was removed from the card. Assistance from the processor is largely calibrated to the correct data feeds a timely and sufficient information on transactions and card loads.

Even established programs with a dedicated in-house risk management team can benefit from what the processor can provide, however, the data and insights processors can provide are typically more comprehensive and real time and in many cases exceed that which individual companies can achieve on their own however, prepaid program managers that don't have this internal knowledge base and core competency are more likely to cede some of this control and will look to their service providers for the expertise of the capabilities that bring them from detection to prevention-based programs. The processor can also provide more regular comprehensive reporting to the program manager compared to that which is completely in-house.

The processor's role in helping to manage fraud starts with the ability to leverage compliance tools in the fraud mitigation process. Processor tools for compliance form the foundation for a fraud management program, as many of the compliance tools are centered on reducing fraud in the first place. Program managers and issuers can work with processors to leverage these tools and expand on them for comprehensive fraud management.

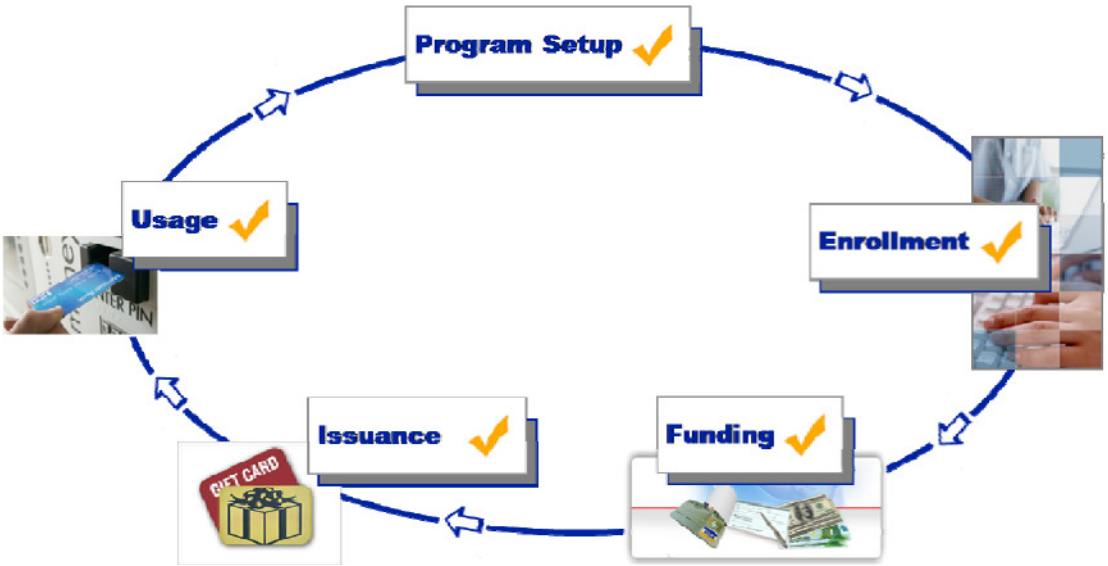
The detection and prevention policies and tools in place include all of the existing card issuance tools prevalent in the card and debit world, such as address validation through public sources verification of cardholder possession of the card as well as several multifactor authentication tools, knowledge based authentication, question-and-answer sets, authorization strategies and scoring, neural networks, and many more. While some of these tools are internally developed at an issuer, they are generally provided by an external service or network provider through either the processor or another program manager partner. The vigilant prepaid processor is integral and setting up the required relationship that allows for additional checks which should include all of the following

- Address verification
- address type
- address high risk match
- change of address
- drivers license verification
- date of birth validation
- phone verification
- phone high risk match
- consumer ID verification (social insurance number)
- Government compliance check or any other regulatory body

Several of the above tools meet compliance requirements, but the additional level of risk mitigation that many also provide cannot be overstated. While they are thought of as detection tools used for non-prepaid products in the course of the transaction on an existing account, they are also preventative tools. Employing the above data elements in your strategies provides the in-depth and calculated capability required in today's sophisticated marketplace.

Financial institutions have a solid foundation of experience in detecting transactional fraud. As credit and debit card issuers, they have recourse: transactional fraud occurs, and depending on the situation at least a portion of fraud losses can be recovered. This scenario changes in the prepaid arena, however, from both banks and non-bank program managers. The complexity of the product set, the nature of the card issuance, and indeed the nature of fraud from the issuer perspective differs greatly. Prevention therefore becomes paramount when managing prepaid risk and fraud

Preventing Fraud Losses



Fraud can hit prepaid accounts at nearly all planes in the product lifecycle. Different mechanisms must be put in place during the program set up to manage fraud that occurs during the enrollment period, when prepaid cards are funded, issued an activated, as well as when they are used at point of sale or ATM. Creating a comprehensive prepaid fraud management program requires the vigilance and experience to effectively deal with this means that if the various points in the prepaid program and product lifecycle and the ability to adjust program parameters as new fraud schemes evolve. The specific instances for the major points of vulnerability can be broken down as follows;

- **Cardholder Enrollment**: the point where the card is purchased or registered. Particularly with the reloadable products, ensuring that the cardholder and buyer are legitimate and authenticated is of paramount importance
- **Card load:** anytime funds are loaded into the prepaid account, and ensuring that they are coming from a legitimate source
- **Card issuance and activation:** the point when the card is created and distributed to the cardholder. Ensuring that the card is received at activated by the actual cardholder is key. With instant issue card this may take place at the time of enrollment.
- **Usage purchase or cash withdrawal activity:** similarly to other card type such as credit and debit, measures must be taken to ensure each transaction is legitimate.

Creating a Network and Ecosystem to Mitigate Fraud

In addition to the prepaid program managers product management team, there are a number of parties with roles in identifying prepaid fraud, reducing losses, mitigating risk in stopping criminals. Many of these are brought to the ecosystem by the processor. The processor forms partnerships with the compliance solution providers, to provide, present and analyze data. Additionally, browser based program management tool should be used to search the prepaid program database when participants discover fraud in order to uncover potentially similar instances. The processor provides analytics on the database to identify the similarities. The network and community created by the processor, issuer and the program manager can include the following pieces:

Processing Product Management

- Works with customers to develop and enhance broad products to meet changing market needs
- Works with processor implementation team, issuer and or program manager to define program fraud systems parameters
- defines the process and ensure his participation of all parties involved
- provide consultation to customers
- provides ongoing support and changes as issuer needs evolve

Dispute Analysis and Support

- Processes cardholder disputes
- may work negative balances were chargeback rights can be enforced
- communicates fraud trends to the group
- often acts as a key contact with law enforcement which can include all levels of enforcement postal inspections to provide research and supporting documentation

Call Center

- Frontline for inbound cardholder requests
- reviews suspicious activity like profile and funding sources update
- creates fraud cases and communicates fraud trends
- conducts outbound calls resulting from broad triggers generated by scoring engines to validate transactions

Fraud Analyst

- Analyzes exception and suspicious activity reports
- works manual or system generated fraud cases and closes fraudulent accounts communicates transactions were chargeback rights may be present to the disputes processing team
- ads confirmed for a profile data to watch lists to prevent further use
- provide feedback on process enhancements to the group
- communicates broad trends to group
- manages transaction scoring engines and the associated fraud rule sets

Compliance

- Provides guidelines for customers interpretation on compliance with regulations
- approved program configuration settings
- key contact with law enforcement and any investigations

Business Partners

- Provides a means of validating data provided. Buyers, card holders and gift givers
- transaction monitoring and scoring

Government Agencies

- Provides regulations with regards to the monitoring and reporting on prepaid accounts

Law Enforcement

- Reviews fraud information provided
- prosecutes criminals

Merchant Acquires

- Processor initiates contact with the merchant acquirer via the network should merchant inside their fraud be suspected

Prepaid Fraud Perpetration

Fraud schemes affect prepaid portfolio managers, merchants that except prepaid cards, and if implemented to a large degree could put a damper on the entire prepaid echo system. Each team seeks to exploit one or more of the vulnerability points through enrollment, card load or purchase cash withdrawal. Common schemes include:

- **Compromise gift card numbers:** in this scheme, fraudsters use software to find valid unregistered gift card numbers, and also to determine if they have value on them. They then register the cards with your address for purchase delivery and use them to purchase either online in collusion with an insider at a legitimate merchant location, or through a fraudulent merchant. The exploitation and assistance is at the point of purchase, generally on line. The program risk manager must work with the issuer and processor to analyze registration of previously anonymous card enrollments to ensure proper transaction parameters are set for the cards, and that the fraudulent transactions are detected as rapidly as possible. In this instance, prepaid issuers generally foot the bill for the loss.

Velocity monitoring on the usage of phone numbers, fraudulent account numbers, addresses, e-mail addresses, etc. is an important tool to combat this type of fraud. The ongoing monitoring of disputed transaction patterns with specific merchants is also important.

- **Force Post transaction:** using a closed prepaid card account, fraudsters through collusion with someone at the merchant, force transactions on the card essentially spending the money that isn't there. This takes the prepaid account into a negative balance. Force Post schemes also have included instances of social engineering where fraudsters learn the procedures followed at a merchant and find ways around it. Unknowingly the merchant may have been tricked into generating a fraudulent force post. Investigations have uncovered instances where the fraudster attempts to buy a big-ticket item with a stolen closed prepaid card number where the plastic has been altered to include a fictitious customer service phone number on the back. When the transaction is declined the fraudster asked for merchants to call the bank for authorization. The merchant is actually calling an associate of the fraudster who was posing as the issuer; that it's okay and give them a false authorization number to force through the system. The fraudster than is allowed to leave with the merchandise. The prepaid issuer is not at risk, as the account is a closed account. Merchants who are not complicit in the fraud do suffer losses and as a result must therefore establish and maintain vigilance about this practice and ensure proper employee training to avoid this type of fraud.
- **Test loads:** fraudsters get a hold of a reloadable prepaid card, call a merchant location posing as the load vendor and need to test the merchants POS system. They give the merchant card number and a dollar amount to load on the card. Once the duped merchant enters the information, funds become available on the card and they are immediately withdraw the cash at an ATM. The merchant takes the loss in this situation. This type of fraud exploits the low transaction vulnerability. Again proper employee training and merchant vigilance can mitigate the risk
- **Stolen Card Loads:** similar to compromise card fraud described above, except in this instance the fraudster uses a stolen debit credit card to find a reloadable prepaid card. The fraudster first needs to add the stole uncompromised credit or debit card to their funding account sources knowing the proper address associated with the stolen card is important to get through address verification service. Most of the time the fraudster uses the stolen card number to fund multiple prepaid cards. Fraud rings also tend to pass the stolen numbers around so that a stolen card may be associated with many different individuals funding account sources. After the fraudster funds reloadable cards they can either take out the cash, buy a gift cards, or buy goods online. By the time the real credit debit cardholder disputes the load transaction the funds are usually gone. The prepaid issuer and/or program manager takes the loss. This type of fraud exploits both the enrollment and the load point's vulnerability. To avoid this fraud requires program managers to monitor low transactions or proactively set limits and take measures to ensure that funds loaded are coming from a legitimate source. Limiting the sources of funding for prepaid accounts is also a viable proactive method of mitigating the fraud.
- **Card reversal fraud:** a fraudulent merchant account is established usually an intranet merchant that will process a credit without having any previous debit transactions. Another example of merchant complicity in prepaid fraud; this type of fraud can be combated with the effective controls and account limits created by using the transaction data supplied by the processor. If the fraud is successful, the issuer program manager takes the loss. This fraud once again exploits the vulnerability at the point of purchase.

Prepaid Fraud Prevention

For each interaction with the cardholder, there are measures that can be taken within the prepaid program to manage fraud. The prepaid fraud mitigation and management process has some key differences to what issuers are accustomed to with credit and debit cards such as preventing fraudulent card enrollment and loads as discussed previously. One similarity common to all card programs is that regardless of who takes the loss in the case of prepaid fraud, be it the merchant, issuer, or program manager each has a distinct motivation to reduce overall fraud. Cardholder confidence in prepaid cards can easily be eroded, causing a reduction in card usage. As this affects all players, each must work to ensure the lowest possible level of fraud throughout the entire prepaid ecosystem and also throughout the entire lifecycle of the program. The following five stages will be analyzed more closely:

1. Program set up
2. Enrollment
3. Issuance and activation
4. Funding
5. Usage

Getting to Prevention: strategy, tactics and processor involvement in program set up

The first step in a prepaid program is to set up. The levels of control, velocity and capacity of loads, access to ATMs, velocity of retail transaction, must be determined and set based on the parameters of the program itself.

This must be coordinated among the program manager, issuer and processor, and continuously reevaluated and recalibrated based on fraud trends, new discoveries and the overall risk that the issuer is willing to bear on the prepaid portfolio. Tools, practices and directives for program set up our as follows:

- Utilize a suite of resources, often provided by the processor, to identify and prevent fraud
- adjust individual program parameters based on risk tolerance levels
- utilize comprehensive real-time and off-line reports often provided by the processor
- compliance considerations
- implement an effective negative balance management plan

What's Being Done Today

The processor is generally the driver for the setup considerations and changes, once the program is up and running.

Fraud prevention at the Enrollment Lifecycle Stage

Prevention of fraud is the most effective, but the least developed aspect of fraud management at the present time. The prepaid risk manager, in conjunction with the processor, must prevent fraud before it even happens, by instituting policies and implementing programs that keep cards out of the hands of fraudsters, much as online merchants need to keep merchandise out of the hands of fraudsters.

Doing so is not always an easy task, but the processor provides tools such as the following to assist:

- Address standardization ensures a valid address and limits returned cards
- reviewing suspicious registration information
- real-time and off-line reports with more breadth of potential fraudulent activity and solely available to the individual issuer
- profile information validated against third-party data
- credit checks

Processors can also assist with the identity and address verification, in reviewing negative files and watch list for prior fraudulent activity on registered accounts, addresses, maintaining card order and purchase thresholds, as well as in the ongoing evaluation of a programs fraud thresholds and fraud checks. This last point is again a continual recalibration of the portfolio based on the latest information changes in fraud schemes and inherent issuer risk. The processor can provide effective insight and guidance on these changes. The prepaid program is ever evolving and should not be subject to static risk parameters. This holds true for enrollment precautions as well.

Effective Risk Management in Card Issuance and Activation

The prepaid world opens up new perspective; especially for financial institutions whose primary approach to risk management was from the debit or credit card issuer perspective.

The prepaid processor must provide coordination and overall guidance to new program managers, as well as those less familiar with the fraud issues specific to prepay. The activation stage of the program is a perfect example. Card issuing financial institutions are accustomed to card activation processes, but not specific to prepaid cards. Processors provide assistance in understanding with regards to this stage on the following fronts:

- Activity on inactive cards
    - at the POS
    - for low transactions
    - balance inquiries
- Activation strategies
    - create a card presence and activation scenario
    - specific cardholder information that leads to more effective cardholder authentication
    - combinations to stay one step ahead of fraudsters
- Maximum card replacement values
- address validation
- Government ID validation
- date of birth validation
- phone verification
- velocity monitoring for address and phone
- card compromise fraud checks

All of the above are examples of how the processor can provide above and beyond the standard use cases, activation scenario and risk mitigation for prepaid issuers. As an example you should require the card to be in hand at the time the cardholder registers the card using the Web interface for activation. Cardholder authentication offers an additional layer of protection from card number generation software and other skimming programs that exploit card not present situations such as online card registration mail-order telephone order and intranet purchases.

The importance of the Valid card Load

The second of are two must haves for effective prepaid fraud mitigation is directly related to the load transaction: ensure that the prepaid account loading mechanism is legitimate, much as online merchants must ensure that the method of payment is not being used in a fraudulent manner.

It is integral for issuers and program managers to move to both the prevention mindset and also the online merchant mindset in dealing with fraud. While the merchant mindset is relatively easy for non-financial institutional program managers to adopt, it may be difficult for financial institutions whose fraud mitigation and compliance groups are crossed pollinated with other products, particularly credit and debit products. Establish prepaid issuing financial institutions may have figured this out, but those who are just entering the prepaid arena could benefit by outsourcing some of the fraud prevention programs to prepaid processors and other partners. The processes that will serve the prepaid community best in the coming years will integrate world-class prevention capabilities that provide effective risk mitigation and also defray the cost to program managers of having such programs in place.

The specific assistance that processors can provide in this arena includes:

- Initial prepaid card purchases
    - address usage
    - funding source usage
    - maximum value limits for a single order
- reloads
    - reloads via single funding source
    - reload value by a single funding source
    - maximum reload value for card
- other load transaction scenarios
    - ACH or EFT transfer high dollar transaction monitoring
    - funding account additions or changes
    - primary account holder address changes signaling a potential account takeover

Mitigating Fraud on Spending Transactions

Last and clearly not least we have the potential for fraud with card usage either at the point of sale or other usage situations. In addition to the fraud prevention techniques and tools inherent to all card transactions that are implemented by merchants, card networks, and issuers, the prepaid processor assists and recognizing suspicious activity and pro actively manages risk and potential losses through the more effective monitoring. Part of this is the implementation of the following:

- Monthly scans providing a linkage between compliance and fraud mitigation
- validation of updates to profile information
- ongoing limit checks
- dispute analysis and support
- credit transaction monitoring and transaction scoring engine integration
- broad trend analysis providing insight and information on the trends that emerged throughout the entire prepaid arena
- engagement in support of law enforcement efforts

Prepaid issuers and program managers generally do not have the breadth of coverage completely and effectively analyze all of the above factors. The prepaid processor provides that additional insight necessary for effective fraud management at the crucial lifecycle point of card usage.

Cardholder involvement in the Fraud Prevention Process

In many instances both the specific fraud types and also with the tools used to combat fraud the value of involving the cardholder as a resource in fighting fraud cannot be over emphasized. Research indicates an even split between fraud which itself detected by the cardholder and that which is detected by a financial institution or third-party. The cardholder as an active participant in fraud mitigation is invaluable in early detection, loss mitigation and in many cases preventing the fraud.

The primary example of this usage of alerts messages sent directly to the cardholder immediately following the transaction, or account balance updates on regular cardholder selected schedules or at some other point in which a change has been made to an account profile. Originally these alerts were more static and not actionable, and sent primarily via e-mail. But the evolution of the mobile channel has presented a stellar opportunity to establish a two-way channel of communication and provide an action on the part of the cardholder that may actually stop fraud in its tracks. Sending text alerts to cardholder's mobile devices in the case of questionable activity and providing the cardholder with the ability to alert the issuer to suspicious activity to prevent further compromise is invaluable. This can be a valuable tool in preventing fraud. When used in conjunction with the limits placed on the account, each individual account can be tailored to specific activity and risk profile.

Conclusion

For processor program manager relationships to reach the next level of effectiveness, program managers must implement solutions that allow for proactive fraud prevention throughout the entire lifecycle of the prepaid program set up to card usage. These include those solutions focused on determining the identity of the buyer of the cards, as well as the validity of the funding source, ensuring that cards don't get into fraudsters hands and that the funds loaded onto the card are not subject to return. Much of these solutions are focused on data sources and cross checks that are often most efficiently run and provided by the prepaid processor. This may entail the ability for program managers to outsource fraud case management, and could have some element of shared responsibility and coordinated fraud mitigation efforts. Should prepaid processors seek out less-developed programs or risk management departments that are strained there is a distinct opportunity for integration and coordination amongst processors, issuers, and program managers. This could also hold true for programs for smaller financial institutions or non-financial institution programs that don't have the same level of risk management expertise as more established programs. Moving forward successfully prepaid program managers and issues will ensure that fraud prevention becomes more and more a part of the risk management component of their prepaid processing services.

The processor can represent an additional line of defense in fraud mitigation. Issuers and program managers must bring the processor into the fraud mitigation process, even though it requires dedicated and extended efforts. The rewards from such efforts could prove to be tremendous. The data that individual issuers and program managers have is not as comprehensive. The insights that can be gleaned from a broader base of data may in many cases exceed that which individual program managers or issuers can achieve. Time and again we see examples of fraud mitigation being enhanced by additional sources of data and information models that gained immense effectiveness simply through the broader perspective provided. Such is the case with prepaid fraud and the involvement of the prepaid processor.