



Prepaid Fraud Mitigation: Leveraging the Processing Relationship to Prevent Fraud Throughout the Prepaid Lifecycle

Conducted by
Javelin Strategy & Research
October 2009

Contents

Introduction	3
Executive Summary.....	4
Working With Prepaid Processors for Comprehensive Fraud Management.....	8
Resolution and Detection: The Backbone of Present Fraud Mitigation Programs	9
Resolution: After the Fact Customer Relationship Management.....	9
Earlier Detection Leads to Lower Fraud Costs	10
Doing it better: How Prepaid Processors Help Mitigate Fraud Further.....	11
Where Does the Core Competency Come From? To Whom Should Program Managers Look for Fraud Mitigation Capabilities?	13
Preventing Fraud Losses Throughout the Entire Prepaid Lifecycle.....	15
Creating a Network and Ecosystem to Mitigate Fraud	16
Prepaid Fraud Perpetration: What are the Most Prevalent Schemes and Who is at Risk as a Result? .	18
Prepaid Fraud Prevention: What’s Being Done Today, Who Does What, what Can be Done Better? ..	20
Managing Fraud Throughout the Prepaid Lifecycle.....	20
Getting to Prevention: Strategy, Tactics and Processor Involvement in Program Setup	20
Fraud Prevention at the Enrollment Lifecycle Stage	21
Learning From the Prepaid Processor – Effective Risk Management in Card Issuance and Activation. .	22
The Importance of the Valid Card Load	23
Card Usage: Mitigating Fraud on Spending Transactions.....	24
Leveraging Cardholder Involvement in the Fraud Prevention Process.....	25
Conclusions	26

Introduction

Prepaid issuance and program management have undergone tremendous expansion, with the largest programs reaching multiple 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 prepaid fraud has the opportunity to blossom – will result in greater trust among prepaid cardholders, greater transaction volume, and more smoothly run prepaid programs.

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 paper 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, the paper provides insight into the future of prepaid fraud mitigation: how prepaid processors are providing additional services and integration into the fraud mitigation process to create a more symbiotic relationship with program managers and issuers.

Executive Summary

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 funds on the card than 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 in dealing with fraud. Established card issuing financial institutions may have figured this out, but those 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 fruition 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 card loads

Prepaid program managers seeking to move to the prevention mindset for fraud will consistently come back to these two principles. The centerpieces of any viable prevention-oriented fraud mitigation

Executive Summary

program will be based on getting as close as possible to making sure neither of the above happen. Preparation is key, and through the combined efforts and vigilance of prepaid processors, issuers, and program managers, growth in prepaid fraud can be proactively 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 transaction and other activity on each account, giving the program risk manager valuable insight and leverage in *detecting* fraud. The relationship and interaction is important, and 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 cardholder and prepaid card purchaser (where necessary depending on product type), and
- 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, change in email address 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 their anti-fraud efforts, 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, intelligence, 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 to 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 (e.g. KYC, AML, OFAC, and other regulatory compliance inherent to all prepaid programs), and the tools the processor makes available for such compliance programs.

Executive Summary

Processors also provide data on card activity – a direct feed, online tools and/or specific reports in the way that prepaid program risk managers need it 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 in 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 anti-fraud 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 in 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 in fraud mitigation – and working with a 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. Though 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. The key in the relationship is defining the needs and capabilities that compliment the capabilities of the program manager. This may be more customized for more established prepaid program managers with robust and developed risk management teams and plans. While new programs, smaller FIs and other program managers may be looking for more of a turnkey processing solution that extends into program and risk management as they must rely on outsourced support or expertise. Even large prepaid issuers that use fraud resources from credit or debit seek a greater understanding of unique prepaid threats. Prepaid processors who focus on fraud provide further insight and this unique perspective.

Executive Summary

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 that 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 in 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.

Working With Prepaid Processors for Comprehensive Fraud Management

Though the prepaid industry has not experienced a major uptick in fraud, vigilance is necessary to proactively 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 transactions 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 (i.e. more funds available once the card is stolen) is that much greater for the fraudster. The ability to both scale transaction volume and also to mitigate fraud is of vital importance for the selection of a prepaid processor. As importantly, fraud reduces profits. With large players such as WalMart cutting fees for prepaid cards, downward pressure on profit margins 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 cards are “good funds” (not subject to chargebacks, and coming from legitimate sources).

Resolution and Detection: The Backbone of Present Fraud Mitigation Programs

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 onto prepaid cards.

It is therefore very important that effective 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. Established prepaid issuing financial institutions with dedicated risk departments 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 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.

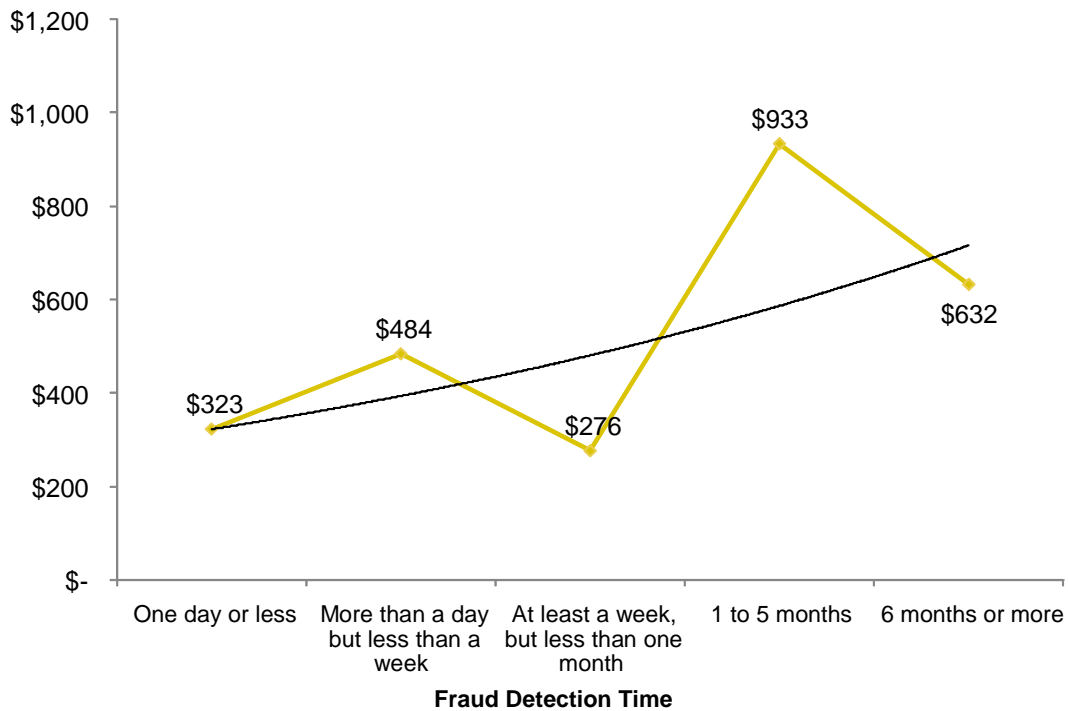
Resolution: After the Fact Customer Relationship Management

Resolution – making the customer “whole” again after fraud occurs -- is important in maintaining the customer relationship, but doesn’t proactively 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 portion 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

Resolution and Detection: The Backbone of Present Fraud Mitigation Programs

cardholder relationships. This makes fraud resolution policies equally important in the prepaid arena. Historically, most prepaid fraud resolution efforts fell with the prepaid issuer and program manager. There is a current trend to more actively involve prepaid processors as well as other third parties in combating fraud thus creating a vested interest in maintaining the ongoing cardholder relationship.

Earlier Detection Leads to Lower Fraud Costs



Q25: From the time the misuse of your information first began, how long did it take you to discover it had been misused? by Q34: How much money did you pay out of pocket as a result of the identity theft?

October 2008, n = 475
 Base: All fraud victims.
 © 2009 Javelin Strategy & Research

Source: "2009 Identity Fraud Survey Report: Identity Fraud on the Rise But Consumer Costs Plummet as Protections Increase.", Javelin Strategy & Research, February 2009

Resolution and Detection: The Backbone of Present Fraud Mitigation Programs

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 among processors, issuers, and program managers is the detection of potential fraudulent activity. The Javelin Strategy & Research Identity Fraud Survey has consistently shown that earlier detection of fraud leads to lower overall losses for all types of existing card fraud.¹ Giving fraudsters less time with stolen account information mitigates fraud. The graph above shows the average out of pocket costs paid by consumer victims of identity fraud as broken down by the time it took to detect the fraud – both the actual numbers and then a statistically smoothed line. The average consumer out-of-pocket cost rises as detection time for the fraud event is extended.² Assistance with earlier detection can affect the overall losses for cardholders, prepaid issuers and program managers.

Detecting fraudulent loads using compromised debit 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 processor to scan their portfolio for other instances where the compromised funding account may be being used. A key control is to establish edit checks to ensure that the funding account information entered, such as name and address, matches the information that is included in the profile of the person who is funding the accounts. Many times these two profiles are different because the fraudster must use the legitimate address of a 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 adds or changes relating to a profile are also important controls to implement with the processor.

Doing it Better: How Prepaid Processors Help Mitigate Fraud Further

In defining risk mitigation strategies and specific tactics, prepaid issuers and program managers 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?

¹ See also: Javelin Strategy & Research, “2009 Identity Fraud Survey Report: Identity Fraud on the Rise But Consumer Costs Plummet as Protections Increase.”

² Ibid.

Resolution and Detection: The Backbone of Present Fraud Mitigation Programs

The data that 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 that 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 in 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 fraud 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 processors that will thrive 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 the 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 transaction processing to an in-depth interaction, particularly with regards to risk management. This is seen in the development of a risk mitigation strategy, in the flow of data from processor to issuer (and 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.

Where Does the Core Competency Come From? To Whom Should Program Managers Look for Fraud Mitigation Capabilities?

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 fraud activity 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 as 65% by implementing proactive preventative measures to stop the fraudulent enrollment and detect the fraudulent load before money was removed from the card. Assistance from the processor is largely calibrated through the correct data feeds of 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 this control and will look to their service providers for the expertise and 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 upon 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 credit and debit world, such as address validation through public sources, verification of

Where Does the Core Competency Come From? To Whom Should Program Managers Look for Fraud Mitigation Capabilities?

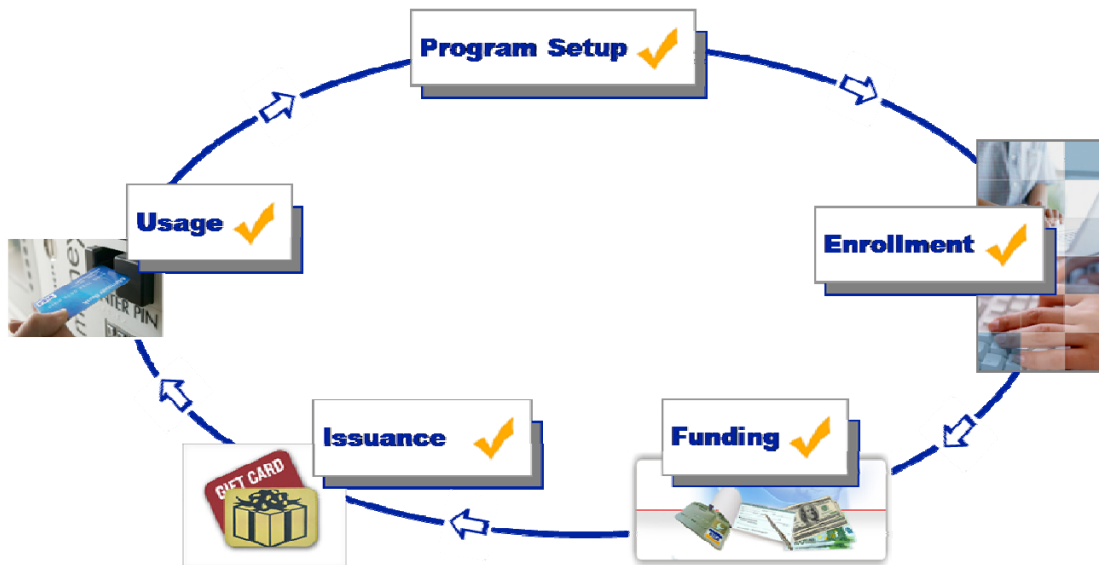
cardholder possession of the card (CVV2/CID), as well as several multi-factor authentication tools, knowledge-based authentication, Q&A sets, authorization strategies and scoring, neural networks, etc. While some of these tools are internally developed at an issuer, they are generally provided by an external service or network provider – either the processor or another program manager partner. The vigilant prepaid processor is integral in setting up the required relationships that allow for additional checks, which should include all 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 (SSN) verification
- OFAC Compliance

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 a transaction on an existing account, they are also prevention 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 portion of fraud losses can be recovered. This scenario changes in the prepaid arena, however, for both bank and non-bank program managers. The complexity of the product set, the nature of "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 Throughout the Entire Prepaid Lifecycle



Fraud can hit prepaid accounts at nearly all points 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 and activated, as well as when they are used at the point of sale or ATM. Creating a comprehensive prepaid fraud management program requires the vigilance and experience to effectively deal with the schemes that hit these various points in the prepaid program and product lifecycle and the ability to adjust program parameters as new fraud schemes evolve.

The specific instances – the major points of vulnerability – can be broken down as follows:

- **Cardholder Enrollment:** the point where the card is purchased or registered. Particularly with 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, 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 and activated by the actual cardholder is key. With instant issuance cards this may take place at the time of enrollment.
- **Usage – Purchase or Cash Withdrawal Activity:** similarly to other card types 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 manager's product management team, there are a number of parties with roles in identifying prepaid fraud, reducing losses, mitigating risk and 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 tools should be used to search the prepaid program database when participants discover fraud in order to uncover potential similar instances. The processor provides analytics on the database to identify these similarities. The network and "community" created by the processor, issuer, and program manager can include the following pieces:

Processing Product Management

- Works with customers to develop and enhance fraud products to meet changing market needs
- Works with Processor Implementation team, Issuer and/or Program manager to define program fraud system parameters
- Defines the process and ensures participation of all parties involved
- Provides consultation to customers
- Provides ongoing support and changes as issuer needs evolve

Dispute Analysis and Support (Processor or Issuer)

- Processes cardholder disputes
- May work negative balances where chargeback rights can be enforced
- Communicates fraud trends to the group
- Often acts as a key contact with Law Enforcement (which can include Secret Service, local law enforcement, postal inspectors, among others) to provide research and supporting documentation

Call Center (Processor or Issuer)

- Front-line for inbound cardholder requests
- Reviews suspicious activity like profile and funding source updates
- Creates fraud cases and communicates fraud trends
- Conducts outbound calls resulting from fraud triggers generated by scoring engines to validate transactions

Fraud Analyst (Processor or Issuer)

- Analyzes exception and suspicious activity reports
- Works manual or system generated fraud cases and closes fraudulent accounts
- Communicates transactions where charge back rights may be present to the disputes processing team
- Adds confirmed fraud profile data to watch lists to prevent further use
- Provides feedback on process enhancements to the group
- Communicates fraud trends to group
- Manages transaction scoring engine and the associated fraud rule sets

Creating a Network and Ecosystem to Mitigate Fraud

Compliance (Issuer/Program Mgr)

- Provides guidelines for the customer's interpretation on compliance with regulations
- Approves program configuration settings
- Key contact with Law Enforcement with investigations

Business Partners (Data validation and transaction scoring engine)

- Provides a means of validating data provided by Buyers, Cardholders and Gift Givers
- Transaction monitoring and scoring

Government Agencies

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

Law Enforcement

- Reviews fraud information provided
- Prosecutes criminals

Merchant Acquirers

- Processor initiates contact with the merchant acquirer (via the Network) should merchant insider fraud be suspected

Prepaid Fraud Perpetration: What are the Most Prevalent Schemes and Who is at Risk as a Result?

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

- **Compromised 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 their 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 in this instance is at the point of purchase, generally online. The program risk manager must work with the issuer and processor to analyze registrations of previously anonymous card enrollments ensure proper transaction parameters are set for cards, and that 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, funding account numbers, addresses, email 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 a merchant, force transactions on the card – essentially spending 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. Unknowing merchants may be tricked into generating a fraudulent “forced” post. Investigations have uncovered instances where the fraudster attempts 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 asks the merchant to call the bank for authorization. The merchant is actually calling an associate of the fraudster who is posing as the issuer, that “it’s ok” and gives them a false authorization number to force through the system. The fraudster then 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, but do suffer losses 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 merchant’s POS system. They give the merchant the card number and a dollar amount to load on the card. Once the duped

Prepaid Fraud Perpetration: What are the Most Prevalent Schemes and Who is at Risk as a Result?

merchant enters the information, funds become available on the card and they immediately withdraw the cash at an ATM. The merchant takes the loss in this situation. This type of fraud exploits the load transaction vulnerability. Again, proper employee training and merchant vigilance can mitigate the risk.

- **Stolen Card Loads:** Similar to compromised card fraud described above, except in this instance the fraudster uses a stolen debit/credit card to fund a reloadable prepaid card. The fraudster first needs to add the stolen/compromised 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 a stolen card may also be associated with many different individuals funding account sources. After the fraudster funds reloadable cards they can then either take out cash, buy 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 points of vulnerability. Avoiding this fraud requires program managers to monitor load 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.
- **Credit Reversal Fraud:** A fraudulent merchant account is established (usually an internet 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 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: What's Being Done Today, Who Does What, What Can Be Done Better?

Managing Fraud Throughout the Prepaid Lifecycle

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 in this paper. Yet 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 be easily eroded, causing a reduction in card usage. As this effects all players, each must work to ensure the lowest possible level of fraud throughout the entire prepaid ecosystem and also throughout the entire life cycle of the program. The following five stages will be analyzed more closely:

1. Program setup
2. Enrollment
3. Issuance and Activation
4. Funding
5. Usage

Getting to Prevention: Strategy, Tactics and Processor Involvement in Program Setup

The first step in a prepaid program is the setup. The levers of control – velocity and capacity of loads, access to ATMs, velocity of retail transactions, etc. – 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 are 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

Prepaid Fraud Prevention: What's Being Done Today, Who Does What, What Can Be Done Better?

The processor is generally the driver for these 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. 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 – more breadth of potential fraudulent activity than solely the information available to the individual issuer
- Profile information validated against third-party data
- OFAC check

Processors can also assist with identity and address verification, in reviewing negative files and watch lists for prior fraudulent activity on registered accounts, addresses, etc., 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 the continual recalibration of the portfolio based on the latest information (changes in fraud schemes and inherent issuer risk, etc.). 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.

Learning From the Prepaid Processor – 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 fraud issues specific to prepaid. 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 and understanding with regards to this stage on the following fronts:

- Activity on inactive cards
 - At the POS
 - For load transactions
 - Balance inquiries (potential indication of fraudulent activity)
- Activation strategies
 - CVV2 (creates a “card present” 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 (address, 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 scenarios, and risk mitigation for prepaid issuers. CVV2 authentication, for example, requires the card to be in hand at the time the cardholder registers their card using the VRU or consumer website. Using CVV2 for cardholder authentication offers an additional layer of protection from card number generation software and other skimming programs that exploit card-not-present situations (for example, card online registration, mail order, telephone order, and internet purchases).

Learning From the Prepaid Processor – Effective Risk Management in Card Issuance and Activation

The Importance of the Valid Card Load

The second of our 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 institution program managers to adopt, it may be difficult for financial institutions whose fraud mitigation and compliance groups are cross-pollinated with other products, particularly credit and debit products. Established 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 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.

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

- Initial prepaid card purchase
 - Address usage
 - Funding source usage
 - Maximum value (limits) for a single order
- Reloads
 - Reloads by a single funding source
 - Reload value by a single funding source
 - Maximum reload value for a card
- Other load transaction scenarios
 - ACH transfer high-dollar transaction monitoring
 - Funding account additions or changes
 - Primary account holder address changes (signaling a potential account takeover)

Learning From the Prepaid Processor – Effective Risk Management in Card Issuance and Activation

Card Usage: Mitigating Fraud on Spending Transactions

Last and certainly 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 in recognizing suspicious activity and proactively managing risk and potential losses through more effective monitoring. Part of this is the implementation of the following:

- Monthly OFAC scans – providing a linkage between compliance and fraud mitigation,
- Validation of updates to profile information
- On-going limit checks
- Dispute analysis and support
- Negative balance management
- Credit transaction monitoring and transaction scoring engine integration
- Fraud trend analysis – providing insight and information on the trends that emerge throughout the entire prepaid arena
- Engagement and support of law enforcement efforts

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

Leveraging Cardholder Involvement in the Fraud Prevention Process

In many of the examples above – 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 overemphasized. Javelin Identity fraud research indicates an even split between fraud which is self-detected by the cardholder and that which is detected by a financial institution or other third party. The cardholder as an active participant in fraud mitigation is invaluable in earlier detection, loss mitigation, and in many cases preventing fraud.

The primary example of this is the usage of alerts – messages sent directly to the cardholder immediately following a transaction, or account balance updates on a regular cardholder selected schedule 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 email. But the evolution of the mobile channel has presented a stellar opportunity to establish a two-way channel of communication, and provide for action on the part of the cardholder that may actually stop fraud in its tracks. Sending text alerts to cardholders' mobile devices in the case of questionable activity (with questionable being defined by the issuer, the cardholder, or both), and providing the cardholder with the ability to alert the issuer to suspicious activity to prevent further compromise. This can be a valuable tool in preventing fraud. When used in conjunction with the limits placed on the account (transaction velocity and amounts, etc.), each individual account can be tailored to a specific activity and risk profile.

Conclusions

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, from setup 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 honed 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 (resource or otherwise), there is a distinct opportunity for integration and coordination among processors, issuers, and program managers. This could also hold true for programs with smaller financial institutions or non-FI programs that don't have the same level of risk management expertise as more established programs. Moving forward, successful prepaid program managers and issuers 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 gain immense effectiveness simply through the broader perspective provided. Such is the case with prepaid fraud and the involvement of the prepaid processor.