**FRAUD**

Fraud is a constant issue of Prepaid Debit cards. Therefore, it is important to be well prepared and equipped to prevent fraud.

The major fraud with Prepaid debit card is during the loading process. Therefore, securing the loading process is key to minimizing fraud. This prevention is done by establishing a strong verification of IDs during the KYC and verifying the loading source.

Another important type of fraud is transactional frauds. To minimize and prevent this type of fraud, the company can rely on an internal team of compliance staff which checks the cardholder’s usage of their cards by relying on reports sent by the processor.

**TYPES OF FRAUD FOR PREPAID DEBIT CARDS**

1. **VALUE LOAD FRAUD**

Value Load Fraud can be as simple as someone using a stolen credit/debit card to purchase the prepaid debit card and load it with money.

**Precautions executed by TransCash:**

When purchases of cards are made at Kiosk locations the agent can verify identification and banks statement to make sure the account belongs to the new potential client. However, when purchases are done online there are no in person screening, therefore here at TransCash the immediate precautionary steps are requesting a scanned image of the clients photo ID and a scanned document of their bank statement showing clearly the Bank logo/name and customer’s name and address. There are also **manual verifications**; such as double checking Billing Address and Delivery Address (if different), personally contacting cardholder through e-mail and phone to verify that they are in fact making the prepaid debit card purchase, checking IP addresses for any discrepancies,

**FIS Tools**

FIS offers a strategy for prevention of value load frauds. The standard featured offered by FIS is an **authorization system** through which all value load transactions must pass.

1. **Negative Files-** FIS keeps a negative database of cards, addresses and phone numbers associated with past fraud and they provide a filter against which new card applicants and value loads may be screened.
2. **AVS- Funding AVS Validation-** accepting XY (street & zip 9 digit/ 5 digit match)

This service provides significant verification confirmation; it validates that the purchaser entered the address that funding card issuer has on file for the cardholder. FIS uses a full match of the address and zip code.

1. **eFalcon-** FIS also uses the eFalcon system to detect fraudulent funding into a client’s prepaid debit card. eFalcon is neural network tool that examines the clients card activity in order to detect any suspicious activity for example commercial billing address. The system can also created behavioral models from which value loads are scored 100 lower risks to 999 higher risks.
2. **RiskWise-** FIS also utilizes RiskWise in order to identify new accounts that seem fraudulent. They captured enrollment data such as; name, address, phone, SSN, DOB and using a list of reasons codes RiskWise provides a verification score. This score can be used to determine the approval decision about opening the new account and shipping a card. Issuers provide their own criteria for scoring and decision.
3. **Octopus-** This tool is used to identify any types of fraudulent activity when funding the prepaid debit card. Octopus identifies all other prepaid debit cards in our portfolio that have been loaded with the same funding card; if any of these debit cards have been identified as fraud then the value load from the funding card will not be permitted to proceed. In addition to funding source, Octopus can perform matches on address and phone number to search for fraudulent cards that match any of these criteria.
4. **DEFRAUDING THE SYSTEM**

Fraudulent customers will attempt to buy the card in order to defraud the system.

**FIS Tools**

1. **KYC-** FIS can provide a secondary validation on high risk address. What this tool does is that it provides a secondary scoring engine for all high risk or failed RiskWise cases.
2. **TRANSACTIONAL FRAUD**

Transactional Fraud happens when there are unauthorized uses of the prepaid debit card due to a card being lost or stolen.

**Precautions taken by TransCash**

As soon as a client informs TransCash that a card was stolen or lost that account is automatically closed and they are issued a new card. However, there can be instances where the client is not even aware the card was stolen or is being used unauthorized.

**FIS Tools**

1. **Authorization Tolerance Factors-** as a preventive tool FIS offers clients the option to specify a tolerance factor for authorizations from selected merchant category codes MCCs where estimated authorizations are utilized such as restaurants, car rentals, hotels etc.
2. **AVS Verification on Purchases Transactions-** FIS supports the AVS for merchants requesting verification for purchase transactions involving prepaid debit cards.
3. **Cardholder Profile Matching-** FIS has the ability to detect multiple or excessive enrollments by a card buyer or card user. The model created based on funding source, scores individuals meeting client-defined criteria for excessive funding sources and for multiple card purchases by the buyer and by the cardholder. The scores are then generated and appropriate action is taken based on the scoring pattern.
4. **Auto-Status Accounts & Auto E-mail Notification-** this is another control method that FIS provides which is the ability to automatically change the status of an account and send an e-mail notification to the buyer or cardholder. Status of card is changed based on the defined criteria in **Falcon, e-Falcon, RiskWise, Cardholder Profile Matching** or **Octopus.** The e-mail will self generate from FIS at the time an account is auto-statused.
5. **Excessive Credit Monitoring- Falcon-** this analysis consists of the identification and assessment of risk on accounts receiving credits (purchase returns) in excess of a specified amount or more than a specified number of credits in a thirty day period. The **Falcon** system is used by FIS in order to detect fraudulent transactions in clients prepaid debit cards. The network examines transactional, cardholder and merchant data to detect a wide range of payment card fraud and then provides a score 0 to 999.

**FIS Tools-**

1. **eRacer-** Electronic Rapid Assessment Capture Environment

This is a proprietary web-based interface used for decision making and analysis of output from the fraud tools. eRacer consolidates all results from all the different detections tools discussed above, in order to review the details of transactions from the prepaid debit card in question. FIS provides direct access to this application providing a unique use ID and password.