

Fraud Management Solutions – First Data Processing Platform

Fraud and Risk Identification Services (FRIS) – A neural network based fraud detection system using cardholder transactions data to create usage patterns and scoring leading to total fraud management including card statusing and fraud case management.

Real Time Auth Decisioning (RT) – Within the FRIS application, transactions can be scored and a decision to block can occur prior to authorization based on a set of parameters set for real-time based authorization decisions.

Risk Management Reporting

Compromised Account Strategies

Auth Blocking – A real time, Internet based, administrative application used to block BINs from foreign currency, country codes, merchant categories, states, or zip codes. Preventive tool sets restrictions blocking authorizations where fraud is suspected or has been detected.

Premium Auth Blocking – An enhanced version of the Auth Blocking administrative application which allows credit unions to block an entire BIN, country code, merchant category, state or zip code with cardholder exclusion or VIP status capabilities.

BIN / Account Limits – Customizable parameters set at daily spending limits for combination of categories such as Cardholder Not Present Limits; ATM; PIN POS; Visa Signature.

Name Mismatching – Track 1 name matching process reviews incoming Track 1 data and compares to cardholder name recorded. Helps in preventing fraud on counterfeit cards.

Address Verification Service (AVS) – AVS is used for transactions occurring in purchased transactions such as phone or mail ordering.

24 Hour Lost / Stolen Reporting

Card Activation – Cardholder activation required upon receipt of a new or reissued card to validate cardholder.

Verification Code Validation – (CVV / CVC and CVV2 / CVC2) – Security codes are used and validated for all cards issued. Thresholds can be set to monitor denials and card statusing.

Verified by Visa (VBV) and MasterCard SecureCode – Internet fraud service requiring cardholders to register their card numbers and choose a PIN for secure online purchases.

FootPrints Online – Internal fraud tool used in monitoring employee data entry via the processor desktop application.

Chargeback processing – Internet application allows for input of disputed transactions to be reviewed and worked by a team of specialists knowledgeable in the chargeback, compliance and arbitration process.

FastData Directory Assistance – As fraud alerts occur and analyst find the cardholder personal information incorrect or unavailable. FastData allows analysts to have increased options available to further search and obtain valid phone numbers for contacting your cardholders.

A98 ATM Initial Keys – To ensure security of ATM keys and to avoid fraud within the ATM Key Initialization System A98 ATM keys, same as DES Keys are now provided electronically instead of previously via hard copy paper format. Only authorized users may request A98 ATM Keys. Electronically format meets the PCI requirements for security.

For more information or to add any of these fraud solutions to your ATM/Debit program contact the ICUL Service Corporation Card Services Department at (800) 304-2273 option 1 and 2.

