

Fraud Management Solutions – FiServ Processing Platform

ENFACT – Neural network used for off line debit card fraud detection system using neural technology to forecast the likelihood of fraud as well as allows credit unions to more effectively manage risk and reduce overall fraud losses through early detection. Product includes case management and near time scoring.

CardTracker – Risk Management tool for tracking compromised cards as identified in Visa or MasterCard alerts. Provides a daily report of all transactions made on compromised cards so a credit union can quickly identify activity that may demand actions to close and reissue.

CaseTracker – Real time web-based application used to monitor, status and interact with eNFACT case activity. This is used instead of waiting for case status reports to arrive next day. Ability to search and download specific criteria, review available transactions associated with specific case, enter actions or review actions taken by analyst, optimized back office process for case resolution, eliminate paper case resolution forms, review demographic details.

TranBlocker – Risk management application that allows credit unions to block and monitor transactions suspected as fraudulent in real time prior to other authorization checks. Available 24 x 7 and accessed through a secure Internet portal, the application is controlled by issuer creating and choosing rule criteria and actions to activate.

Risk Management Reporting

Compromised Cards – Web-based management tool that allows credit unions to search and retrieve compromised card alert information including downloading the card numbers effected by the alert. Based on search criteria that are set by the credit union, the system can download compromised card numbers for use by the credit union to management and take appropriate action.

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

24 Hour Lost / Stolen Reporting

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

Risk Office – Through this product, CU's can have access to an investigation center working directly with fraud analysts receiving real time and end to end incident management of fraud. Determine appropriate strategies to mitigate exposure.

Enhanced Chargeback Service - Assists clients in chargeback processing in regards to selection of chargeback reason codes, creating and gathering supporting documentation, managing timeframes and recommendations for arbitration.

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.

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

Velocity Checks -This feature would monitor the frequency of card usage. A recent fraud technique includes initiating multiple, small dollar transactions with the initial CVV/CVC set to 001. The CVV/CVC value is then incrementally increased by a factor of one, until the correct CVV/CVC value is identified. Adding denial and inquiry transactions to the velocity would also identify a fraud situation earlier.

Name Matching -This feature compares the cardholder name transmitted on the Track 1 mag stripe to the name stored on each cardholder record on the CNS | EFT system. The issuer has the option to denying the transaction based on a mismatch, similar to expiration date mismatching. All mismatches will be reported.

CVV/CVC Checks on all Transactions -In situations where the Track II information is transmitted and CNS | EFT stores the CVV/CVC values, the CVV/CVC values will be validated for all transactions, including PIN transactions. The issuer will have the option of denying the transaction based on a mismatched PIN transaction. All CVV/CVC mismatches will be reported.

Daily Account Alert – This report is used to access the scores that best detect fraud

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

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.