Enacomm®

Bringing Intelligence to Customer Self-Service

More Than a Million Times a Day

eFraud Control MODULE

ENACOMM Fraud Control Module – Identify, Track and Act

Fraud control has traditionally focused on point of sale, not customer service. ENACOMM's Fraud Control Module (FCM) addresses fraud occurring in customer servicing channels, before Point-of-Sale.

The ENACOMM Fraud Control Module protects your customer servicing applications from fraud and money laundering activities by tracking customer behavior in real time across IVR, Web, and Mobile servicing channels. FCM analyzes all customer interaction details, automatically identifies potential fraud, classifies it, and alerts on the findings. A complete end-to-end Fraud system – APIs, reporting, analyst workflow, detection, notification, and prevention measures in one application!

Fraud Rule is Violated → **FCM Notifies Client** → **Action Sets Deployed** → **Fraud Prevention & Resolution**

CLIENT BENEFITS

- Monitor servicing interactions in real time by IP address, account number, or ANI
- Set up whitelists to avoid false positives and blacklists for known fraudsters
- Configurable rules engine detects fraud rule violations based on your risk indicators and tolerance
- Stop "fast burn" and "slow burn" brute force attacks
- Customizable action sets give fraud teams automatic multi-dimensional fraud detection and prevention responses
- Checks existing customer sources and account numbers against white lists, suspected fraud, and confirmed fraud lists to determine how to best treat the customer
- Tracks and responds to behaviors such as excessive call center transfers, unwarranted IVR use, card entry errors, and use of telephony and IT resources

PROVEN FRAUD PREVENTION

- Protect accounts that receive servicing requests from multiple ANIs or IP addresses
- Ensure J-hook products are not compromised before being purchased
- Expose fraudsters that spoof or otherwise manipulate their phone number or come from suspicious IP addresses
- Catch key account activity across servicing channels such as multiple PIN changes, account takeover, replacement cards, card-to-card transfers, and more
- Automatic fraud rule violation action sets allow for Fraud Analyst intervention, forwarding to "honeypot," hanging up, message playback, limiting application functionality, and more

Interested in learning more?

Please reach out to an ENACOMM business development resource or visit our website.

salesinquiries@enacomm.net • 918-858-9777 • www.enacomm.net