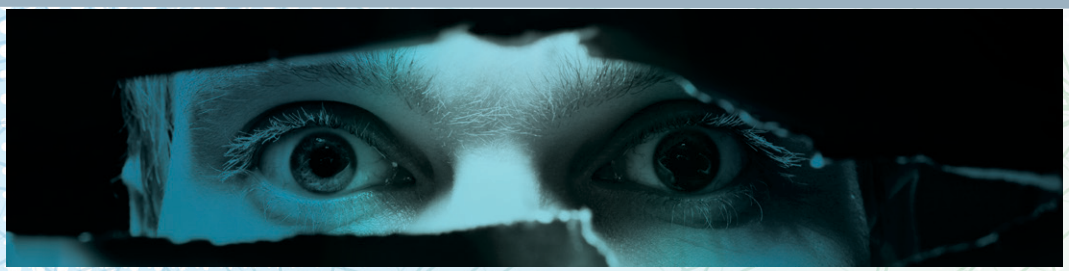
enacomm®

eFraud Control MODULE

Protect Your Systems and Customers with the ENACOMM Fraud Control Module



Every Fraud/Risk professional in the payment card industry needs to be concerned with these 5 fraud schemes that leverage the IVR Channel

	Scheme	Behavior in the IVR	Preventative Action
1	Mining for valid customer card numbers & personal information to test data prior to a social engineering attack or a fraudulent transaction across other channels	High velocity of calls from the same ANI or spoofed ANIs with large number of validation errors Example: 1,500 calls on a single customer credit card in extremely short time frame "Low and slow" attack pattern to avoid detection that presumably leverages bots which often use same 8 digits of an ANI & increment just last two digits	Spoofed ANIs & valid ANIs with high call counts, long talk times, high velocity of validation errors can be transferred to special agent queue, blocked, or reported to Fraud/Risk department If high velocity on a valid card, that card should be suspended or blocked
2	Criminal has obtained stolen card numbers & PI from social engineering, dark web, or other elicit means Use same ANI or numerous spoofed ANIs to test for valid Cards & PI through IVR Channel When target is identified, PIN is changed & fraudster empties account	Single ANI or multiple - spoofed ANIs accessing multiple cards & resetting pins on multiple cards in IVR or through other self-service channels	Proactively identify suspicious ANI Allow the fraudster to enter the card number and stolen PI data, which notifies the Fraud/Risk department to suspend or block card and/or notify card holder Prevent pin changes or other high risk transactions such as card to card transfers from being facilitated in the IVR & other omni - channels
3	Fraudsters using the IVR channel to "shop" for large balance targets for account takeovers Takeover happens in other customer service channels	High velocity of balance inquiries with same ANI or spoofed ANI across multiple cards & sometimes on same phone call	Identify high velocity calls Capture card numbers identified for review and action by Fraud/Risk department. Suspend or block cards associated with these behaviors
4	Known fraud & money laundering "rings" transacting with the IVR for unknown purposes	Callers calling the IVR from known blacklists	Block these call types at the carrier level
5	Fraudsters use a SIP phone device to instigate Telephone Denial of Service (TDoS) attack to bottle neck the IVR & apply pressure on CSRs so they can use social engineering to obtain PI data	High volume of calls to the IVR from overseas and/or unverifiable ANIs	Block these call types at the carrier level

For more information contact ENACOMM at **salesinquiries@enacomm.net** or **877-860-0025** and ask for **Sales**