enacomm®

Bringing Intelligence to Customer Self-Service

More Than a Million Times a Day

Fraud Control MODULE

CASE STUDY

Why Do I Need a Fraud Control System?

Maria, VP of Security, was tasked with finding out if the IVR system utilized by her bank was becoming a target of fraud. The bank was concerned that attackers were looking to attack IVRs as the channel of least resistance due to the bank's focus on major channels of monetary loses, such as data centers, data networks, and the plastic cards themselves.

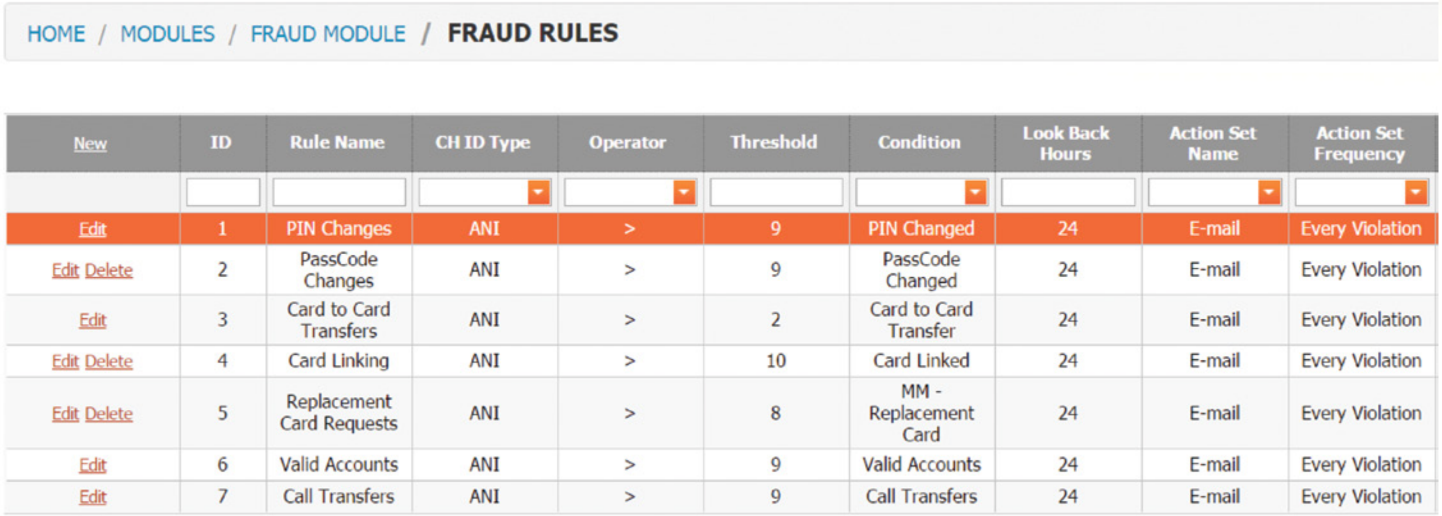
Maria approached ENACOMM for help identifying behaviors within the IVR applications that could be indicators for fraud, and insight into behavior within those areas that could be viewed as questionable.

ENACOMM implemented the Fraud Control Module (FCM) to begin monitoring the IVR functions that could be exploited for fraud. FCM continuously reviewed the actions of every caller, and compared the call events against predefined rules of behavior. When a caller violated a rule, FCM logged the offending caller to the FCM system for tracking, and sent an alerting e-mail to the bank personnel advising them that a rule had been violated. The banking personnel could then access the FCM system to review the specifics about the violation and all other calls made by the caller in question.

As violations were confirmed as fraudulent, call restrictions were put in place by the bank's personnel using the FCM system that either restricted functionality, or blocked the caller completely on future calls.

Maria and her team came up with seven caller behaviors that they determined could be used to commit fraud. Fraud Rules within the FCM system were then generated for FCM to use for monitoring.

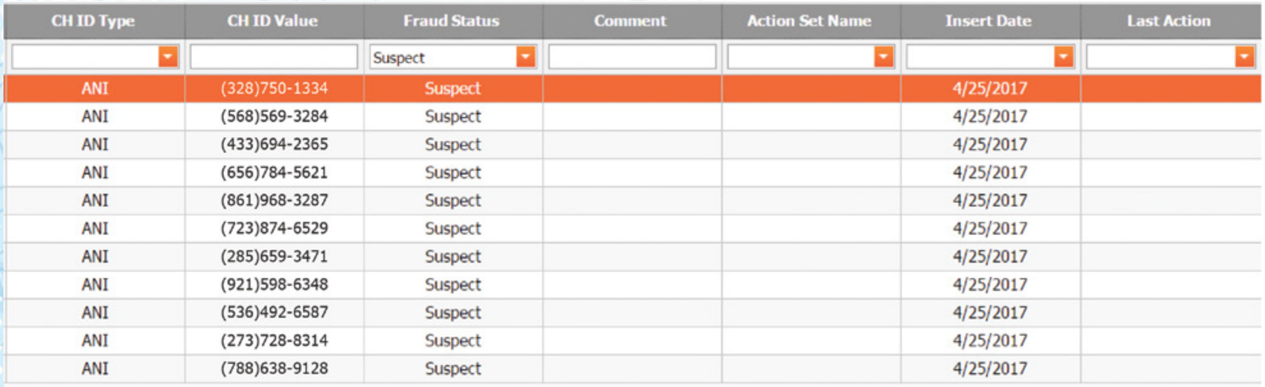
Fraud Rules



HOME / MODULES / FRAUD MODULE / **FRAUD RULES**

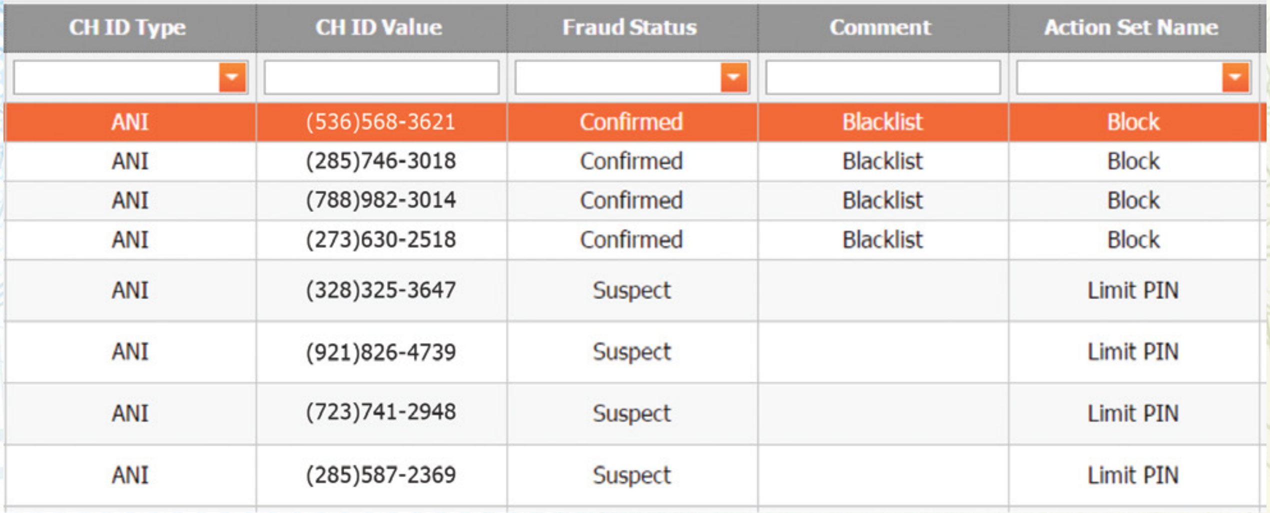
New	ID	Rule Name	CH ID Type	Operator	Threshold	Condition	Look Back Hours	Action Set Name	Action Set Frequency
Edit	1	PIN Changes	ANI	>	9	PIN Changed	24	E-mail	Every Violation
Edit Delete	2	PassCode Changes	ANI	>	9	PassCode Changed	24	E-mail	Every Violation
Edit	3	Card to Card Transfers	ANI	>	2	Card to Card Transfer	24	E-mail	Every Violation
Edit Delete	4	Card Linking	ANI	>	10	Card Linked	24	E-mail	Every Violation
Edit Delete	5	Replacement Card Requests	ANI	>	8	MM - Replacement Card	24	E-mail	Every Violation
Edit	6	Valid Accounts	ANI	>	9	Valid Accounts	24	E-mail	Every Violation
Edit	7	Call Transfers	ANI	>	9	Call Transfers	24	E-mail	Every Violation

Once the alerts were generated when a violation occurred, the offending ANI was inserted into the Fraud Management table allowing the bank to review the actions of the caller and determine if restrictions should be put in place.



CH ID Type	CH ID Value	Fraud Status	Comment	Action Set Name	Insert Date	Last Action
		Suspect				
ANI	(328)750-1334	Suspect			4/25/2017	
ANI	(568)569-3284	Suspect			4/25/2017	
ANI	(433)694-2365	Suspect			4/25/2017	
ANI	(656)784-5621	Suspect			4/25/2017	
ANI	(861)968-3287	Suspect			4/25/2017	
ANI	(723)874-6529	Suspect			4/25/2017	
ANI	(285)659-3471	Suspect			4/25/2017	
ANI	(921)598-6348	Suspect			4/25/2017	
ANI	(536)492-6587	Suspect			4/25/2017	
ANI	(273)728-8314	Suspect			4/25/2017	
ANI	(788)638-9128	Suspect			4/25/2017	

After reviewing the caller behavior, the bank was able to move the offending ANI to a "confirmed" status and choose the limitations they wish to impose on the caller, up to blocking the caller from the IVR all together.



CH ID Type	CH ID Value	Fraud Status	Comment	Action Set Name
ANI	(536)568-3621	Confirmed	Blacklist	Block
ANI	(285)746-3018	Confirmed	Blacklist	Block
ANI	(788)982-3014	Confirmed	Blacklist	Block
ANI	(273)630-2518	Confirmed	Blacklist	Block
ANI	(328)325-3647	Suspect		Limit PIN
ANI	(921)826-4739	Suspect		Limit PIN
ANI	(723)741-2948	Suspect		Limit PIN
ANI	(285)587-2369	Suspect		Limit PIN

Maria and her team were fairly confident that FCM would support their belief that minimal fraudulent activity was occurring with the IVR. However, during the first week of use, the FCM system alerted the bank to 200+ callers that violated business rules. Maria was quoted as saying that "FCM opened our eyes to the fraud attacks that were going on in the IVR, and now gives us a way to identify and stop the attacks".

The ENACOMM Fraud Control Module (FCM) is a modular application that directly integrates with the ENACOMM ViA reporting system. Overall, this dedicated module implements customizable fraud indicators to identify, report, and take definitive actions regarding suspected fraud. While the FCM is not a fraud prevention tool in the same manner as biometric authentication or other point of access tools, the FCM is a powerful way to discover fraud, to learn the latest tricks being used by fraudsters and to electively take action and to provide the information you need to establish effective countermeasures.

IT'S ALL IN THE DATA.

Typically, every call you receive has 30 to 50 details describing every step the caller took in the IVR. If your organization receives 12 million calls a year, the results could be 600 million unexamined details of customer data. Can you really afford not to analyze this data? By examining those details in real time, the ENACOMM FCM identifies potential fraud, classifies it, and reports the findings. Depending on business rules, the FCM system also will activate a variety of actions.

enacomm®

Fraud Control MODULE

Corporate Headquarters: Tulsa, OK
Sales/service offices and data centers strategically located across the United States

918.858.9777 • 877.860.0025
salesinquiries@enacomm.net • www.enacomm.net