Identify, Track & Respond To Fraud Across Multiple Customer Servicing Channels.

eFraud Control MODULE

Bringing Intelligence to Customer Self-Service

Millions of Times a Day

enacomm®

Fraudsters Are Attacking Your Servicing Channels Every Day. Can You Respond?

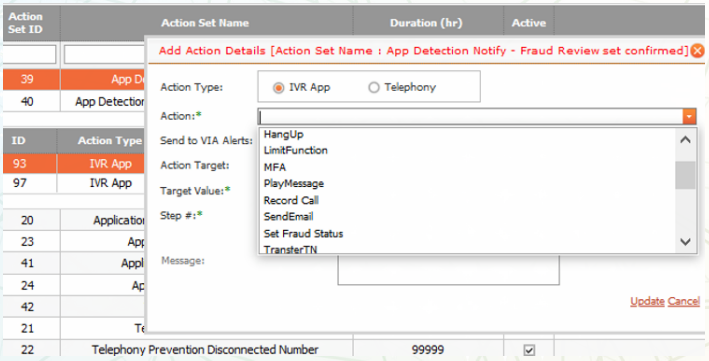
PROTECT YOUR IVR, WEB, MOBILE SERVICING CHANNELS AND CUSTOMERS WITH THE ENACOMM FRAUD CONTROL MODULE

Face it, fraudsters are using your servicing channels every day. Whether obtaining PIN numbers by brute force, attempting to launder money, activating too many cards or taking advantage of your scheduled maintenance periods, fraudsters are focused on stealing from you and your customers or using your financial institution for their illicit activities.

For example, 85% or more of your IVR traffic is probably contained to the IVR — never being transferred to an agent — and does not have the appropriate fraud detection, tracking and prevention your organization needs. It is this "invisible" fraud that may be costing your organization hundreds of thousands of dollars — or even millions. Plus, internal cost cutting programs are now driving more and more at-risk activities to self-service, resulting in an even greater risk of fraud.

THE ENACOMM FCM DETECTS, TRACKS AND ACTS!

The ENACOMM Fraud Control Module (FCM) directly integrates with the ENACOMM ViA reporting system. The FCM provides standard and customizable servicing application fraud indicators to identify, report and take preventative actions regarding suspected fraud. The FCM is a powerful way to discover fraud, to learn the latest tricks being used by fraudsters and to optionally take action to automatically create and enforce effective prevention measures. FCM is the only complete servicing fraud system on the market – APIs, logging, work flow, detection, notification and prevention measures in one application!



User Definable Action Sets Determine Next Steps After a Fraud Rule Violations.

IT'S ALL IN THE DATA.

Typically, every customer service interaction has 25 to 75 details describing every step the customer took. If your organization receives 12 million servicing interactions a year, the results could be 600 million or more details of unexamined customer data. Can you really afford not to analyze and act on this information?

By examining those details in real time, the ENACOMM FCM automatically identifies potential fraud, classifies it, and reports the findings. Depending on defined workflow, the FCM will then execute a variety of detection or prevention actions.

Our Fraud Rules Engine Controls Activities and Actions.

Select ALL Rows | Delete Selected Rows

New	ID	Rule Name	Rule Type	CH ID Type	Operator	Threshold	Condition	Look Back Hours	Action Set Name	Action Set Frequency	Active	Action Count
Delete Edit	86	Accessing Closed Cards	IVR App	ANI	>=	2	Closed Account - Charge Off	4	App Detection Notify - Fraud Review	Every Violation		0
Edit	53	ANI Spoof	Telephony	ANI	=	1	InvalidEOC	0	Telephony Prevention Block	Every Violation	✓	3
Edit	51	Call Velocity	Telephony	ANI	=	1	Call Velocity	0	Telephony Prevention Block	Every Violation	✓	7
Delete Edit	71	Card Not Found	IVR App	ANI	>=	5	Card Not Found	4	App Detection Notify - Agent Review	Initial Violation		0
Delete Edit	57	Default	Telephony	ANI	=	1	Other	0	Telephony Prevention Block	Every Violation	✓	0
Delete Edit	74	Excessive PIN Changes	IVR App	AcctNum	>=	4	PIN Change	4	App Detection Notify - Agent Review	Initial Violation		0
Edit	87	Excessive Stolen Cards	IVR App	ANI	>=	4	Answered Calls	1	App Detection Notify - Agent Review	Initial Violation		164

Fraud Control Has Traditionaly Focused on Point of Sale, Not Servicing.

FCM IS ALWAYS ACTIVE, ALWAYS LISTENING.

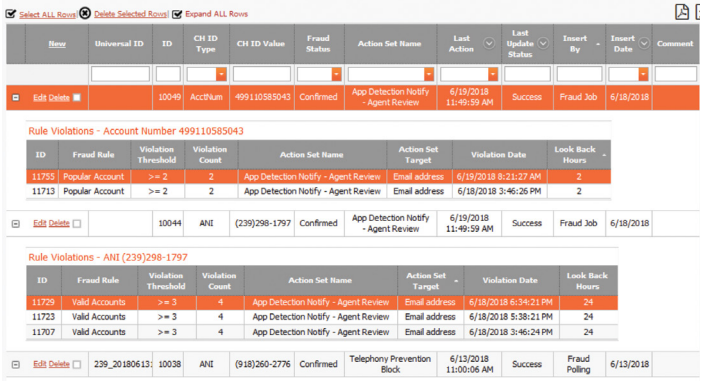
The FCM benefits both your fraud and compliance groups. Whether you're identifying and tracking card holder fraud or suspected money laundering through suspicious funds transfers, the ENACOMM FCM is constantly analyzing all interactions in real-time, reporting suspected fraud, and taking a variety of actions. Overall, the system:

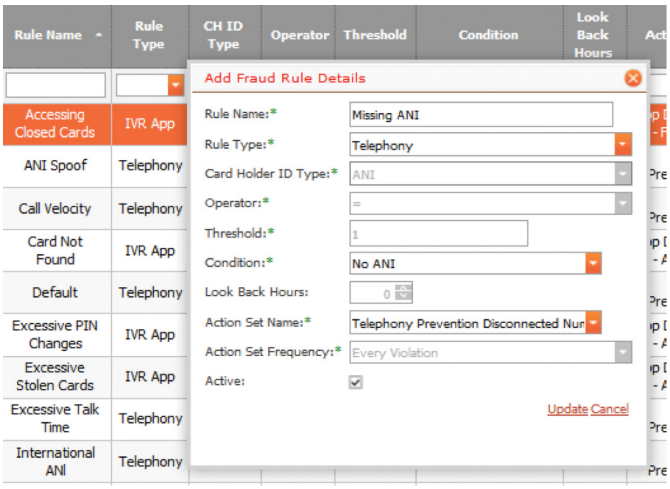
- Evaluates servicing interactions in real-time using the caller's ANI, IP address, device ID or account number and compares their activity to preset business rules.
- Analyzes historical customer interaction records to identify and record potential fraud.
- Checks existing customer sources and account numbers against white lists, suspected fraud, and confirmed fraud lists to determine how to best treat the customer.
- Tracks and responds to behaviors that waste your company's resources such as excessive call center transfers, unwarranted IVR use, excessive card entry errors, and excessive use of telephony and IT resources.

FRAUD RULE EXAMPLES:

- The source is spoofed
- The ANI is invalid or missing.
- One card number is accessed by four or more sources.
- Three or more card numbers are used by the same source.
- Three or more card-to-card transfers are performed by the same across multiple channels within one hour.
- Four or more PIN change attempts across four unique cards are performed by the same source over a 48 hour period.
- Three or more card replacements are requested by the same source.

All Fraud Entries Include a Complete Record of All Violations and Actions Taken.





Fraud Rules Can Be Customized To Your Needs.

- Four or more card linking requests are made by the same ANI.
- Five or more authentication failures for the same card.
- A caller has more than 2 hours of talk time in a 12 hour period.
- The proxy is a T or exit.

These fraud rules can then automatically trigger action sets that may include:

- Blocking the call at the telephony carrier.
- Re-routing the caller at the telephony carrier.
- Asking the customer for additional authentication information.
- Checking the customer's interaction source (ANI, IP address, device ID) for known fraud indicators.
- Limiting the caller's functionality in the servicing application, such as prohibiting funds transfers.
- Playing messages, transferring the call to the call center, displaying pages.
- Moving the fraud entry to the confirmed fraud queue.
- Sending a text and/or email, alerting the risk management and/or fraud groups.
- Hanging up/disconnecting.
- Acting in any combination of the above.

Plus, the FCM can detect international and spoofed sources which may be attempting brute force attacks or a denial of service attacks. Even if the interactions are nuisance interactions and not fraudulent, they may be costing you thousands of dollars per day in IT, telephony, and IVR costs and should be stopped.

Suspected Fraud Work Queue Allows Analysts to Quickly Evaluate New Fraud Entries and Rule Violations.

The Comprehensive ENACOMM FCM Feature Set.

REPORTING AND DATA RETENTION:

- Actions taken during an interaction in response to a fraud rule violation are recorded in ViA reporting.
- At-a-glance fraud entry and rule violation counts.
- Includes standard ViA Fraud Call Count, Fraud Rule Summary, and Fraud Rule Violation reports.
- All fraud entry tables can be exported to XLS or PDF files.

INTEGRATED TECHNOLOGY:

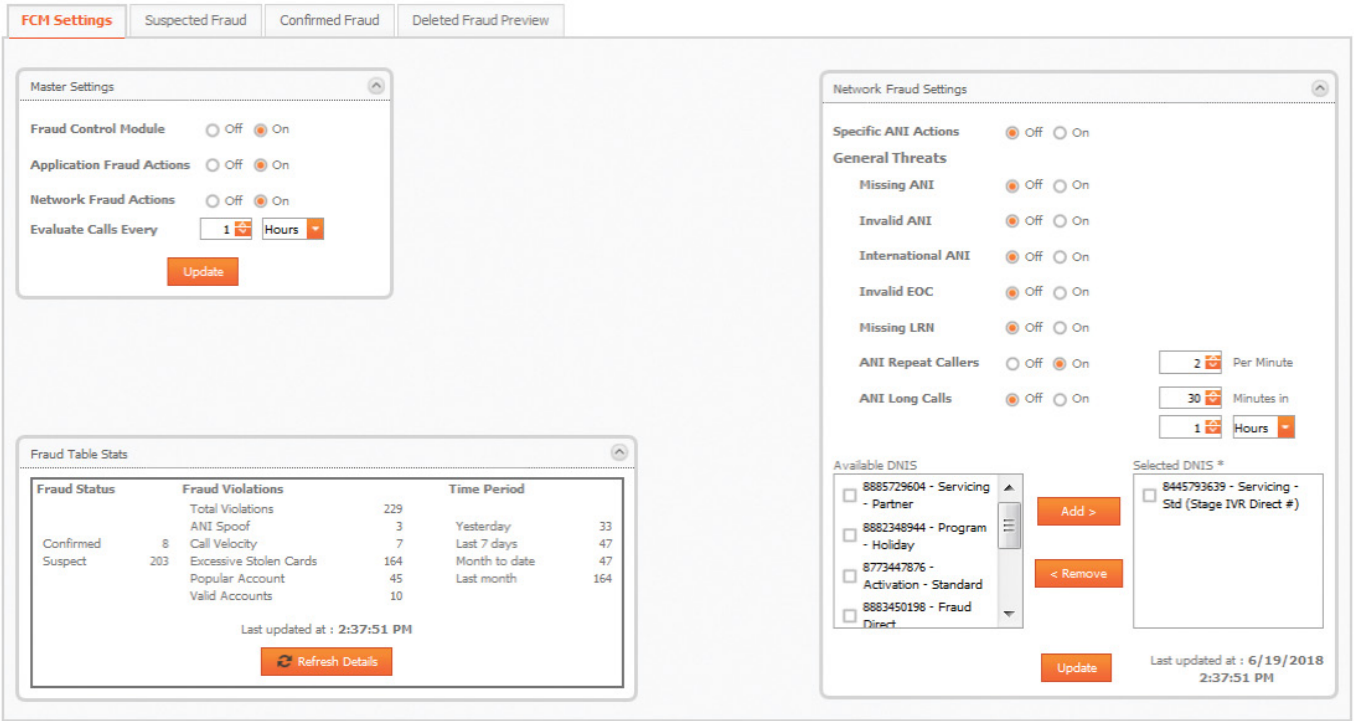
- FCM is accessed through the ENACOMM Engage portal.
- FCM displays suspect and confirmed fraud entries and associated violations allowing risk/fraud groups to manage the fraud entries.
- FCM is integrated with ENACOMM's ViA customer interaction, reporting, monitoring and alerting application.
- FCM provides a fraud analyst workflow framework.
- Imports your existing fraud and white lists quickly and easily.

AVAILABLE FCM API CALLS:

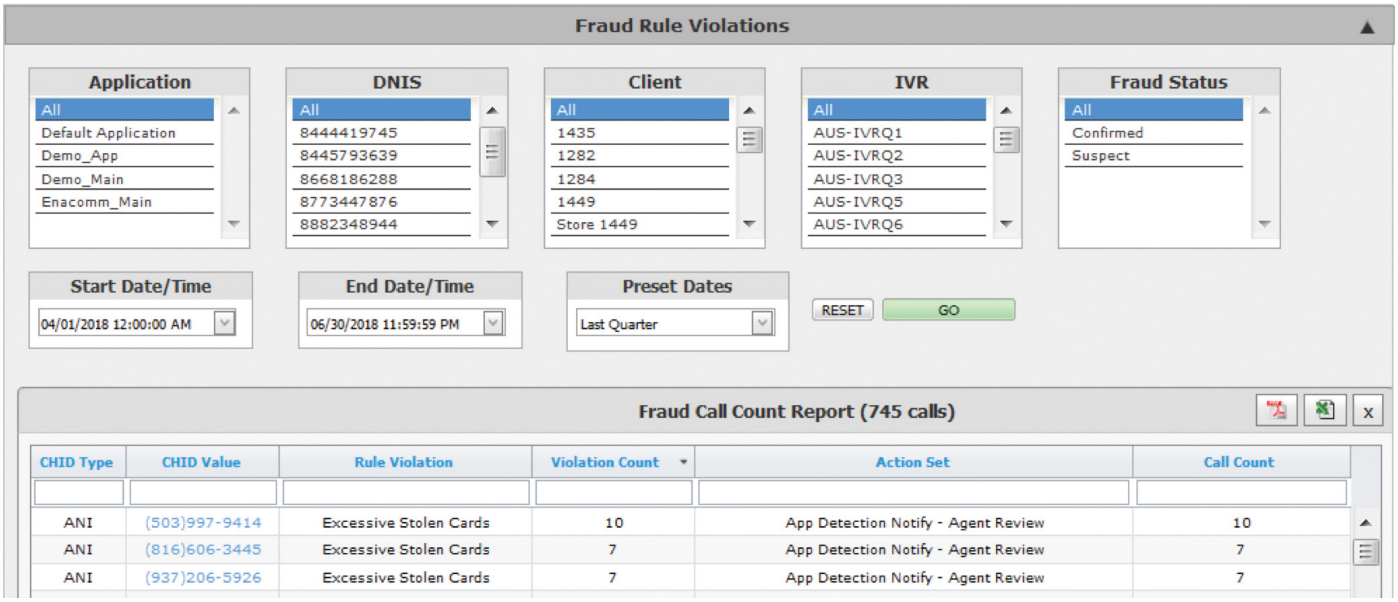
- ANI Spoof Detect
- Reverse ANI Lookup - owner, carrier, port status, line type and more
- Reverse IP address lookup - location, domain name, company name, proxy and more
- Source and Account FCM status - white list, suspect, confirmed, assigned actions
- Interaction Logging - interaction start, end, date/time, application, source, destination, end reason, company, server name, account number, and more

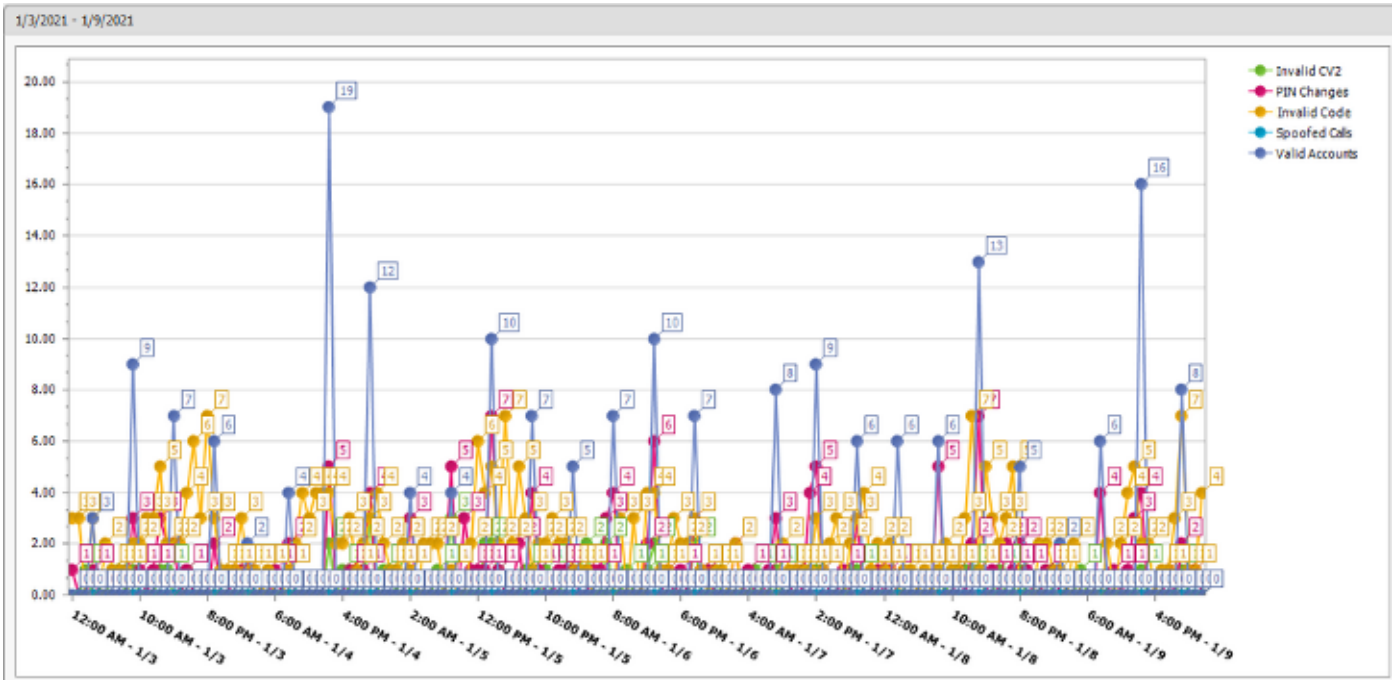
The Fraud Management Console Provides a Quick Overview of System Status and Activity.

Fraud Managment Console



Detailed Fraud Rule Violation Reports Provide Valuable Insights to Help You Design Effective Counter Measures.





Customizable Fraud Detection and/or Prevention Action Sets.

Action Set

Action Set ID	Action Set Name	Duration
20	App Detection Notify - Agent Review	1
14	App Detection Notify - Fraud Review	96
24	Application Prevention - Limit PIN Options	72
23	Application Prevention - Xfer To Fraud	24

Add Action Details [Action Set Name : Application Prevention - Xfer To Fraud]

ID: 42, 41, 1, 21, 22, 28, 27

Action Type: IVR App / Telephony

Action:*

Send to VIA Alerts:

Action Target:

Target Value:*

Step #:*

HangUp
LimitFunction
None
PlayMessage
SendEmail
SendSMS
TransferAG

FCM Provides ANI and IP Address Reverse Source Lookup To Assist Analyst Research.

Action Set | App Detection N

56

Type	CH ID Value
I	(254)2
I	(260)4
I	(312)4
I	(434)2
I	(502)9
I	(513)2
I	(513)2

Reverse ANI Lookup Results

PHONE
Number: 4342 [redacted]
Number2: (434) [redacted]
Status:
DNC:
Type: CELLULAR
Voip:
Carrier: VERIZON WIRELESS
OCN: 6827
Ported:
SmsEmail:
State: VA
Location: LYNCHBURG
LATA: Lynchburg VA
TimeZone: EASTERN STANDARD TIME (EST)
TimeNow: 1/7/2021 2:30:46 PM
Code: LOC

Copy to Comments | Close

Users May Define Contact Lists to Receive Fraud Notifications.

CALL 1-877-860-0025 TO ARRANGE A DEMONSTRATION. ASK FOR SALES!

eFraud Control MODULE

enacomm®

Bringing Intelligence to Customer Self-Service

Millions of Times a Day

Bringing Intelligence to Customer Self-Service

Millions of Times a Day

Corporate Headquarters: Tulsa, OK

Sales/service offices and data centers are strategically located across the United States

918.858.9777

877.860.0025

salesinquiries@enacomm.net

www.enacomm.net

ENACOMM is PCI-DSS certified and approved by the major payment networks.

ENACOMM® and the ENACOMM Fraud Control Module™ (FCM) are registered trademarks of ENACOMM, Inc.
ViA® name and mark are registered trademarks of Call Analytics, Inc.

©2021 v0318V9