Integration Guide for EnScreen ESP Real-Time Fraud Monitoring Schemes for Global FSI Online Fraud

Proprietary and Confidential

Navaera Sciences, LLC

August 24th, 2020

Table of Contents

The remainder of this page was intentionally left blank

1. Introduction

Navaera On-Demand Real Time ("NOD-RT") is a real-time event stream processing solution that enables card, cheque, and other electronic transactions to be monitored in real-time; empowering subscribing institutions to react with greater speed to mitigate fraud or mass compromise attacks.

Navaera maintains a series of analysis modules, or 'schemes' that monitor for both previously seen, and previously unseen fraud behavior. Schemes are designed to identify transaction patterns that indicate known fraudulent behavior, or 'Red Flags.'

Navaera subscriptions or leases include different packages of analysis schemes that may vary by subscription type or level.

This document discusses basic integration for NOD-RT online financial access and transaction monitoring. In this document, we will overview typically implemented fraud schemes, review typical data population, and also review the structure of a typical key-value pair tuple.

This document is not designed to provide detailed rule logic, or discussion on fraud monitoring coverage. Rather, it is designed to discuss typical implementation for data exchange, and basic monitoring. It should be noted that custom development of tuple structures or monitoring schemes is possible within the EnScreen ESP or NOD-RT solutions.

This document only covers real-time monitoring. Batch monitoring for preventative fraud and anti-money laundering monitoring are based on different solutions, and have different implementation requirements.

The following sections of this document discuss scheme options, data model support, and tuple structures.

2. Fraud Monitoring

The following schemes have been specifically created to monitor online banking transactions for fraudulent activity. Online banking transactions can be conducted for a multitude of locations and purposes. Using a series of specifically targeted filters and rules, transactions are scrutinized on a variety of levels for irregular activity by the member/customer or merchant. The following sections of this document will discuss global filters, and transaction rules.

2.1 Global Filters

The vast majority of transactions conducted by an FI do not involve fraud. The quicker that a transaction can be identified as not meeting a fraud typology and approved greatly improves the efficacy of the fraud monitoring process. Global Filters are rules which are applied to specific fields to identify very low risk transactions that should be approved without further review. These rules are applied on a single or a combination of fields which allows for a quick approval of the transaction.

Scheme Code	Scheme Short Description	Scheme Analysis Description
GF001	Global Filters	Identifies transactions that meet specific thresholds or parameters that allow automatic approval of a transaction without further monitoring.

2.2 Authentication Level Rules

The example rules below apply to details of the customer/member's session with the online banking or financial transactions platform.

Scheme Code	Scheme Short Description	Scheme Analysis Description
ORT001	IP Geo Mismatch	Detect and identify when device time zone and geo location of the IP address are different.
ORT002	Proxy True IP Mismatch	Detect and identify when there is a mismatch between the Proxy IP and the True IP.
ORT003	High Risk Account Creation	Detect and identify when online account creations coming from suspicious ISP or IP. A risky ISP or IP List is maintained for monthly, quarterly or yearly reviews.
ORT004	Multi Time Zone per User per day	Detect and identify when a user is linked to multiple time zones per day.
ORT005	Inverse IP Geo Mismatch	IP Geo location is Canada but device time zone is of a high-risk country.
ORT006	Login from Multiple Countries	Identifies customers who login to their account from multiple countries within a specific time window.
ORT007	Login from Blacklist IP Address	Identifies customers who have attempted logins from blacklisted IP addresses.

2.3 Transaction Level Rules

This section provides a list of example rules that are applied at the time a financial transaction is conducted. The goal is to quickly identify if the transaction meets a specific online fraud typology and make a decision as to how to move forward with transaction processing.

Scheme Code	Scheme Short Description	Scheme Analysis Description
ORT008	New Customer Access	Identifies customers who are newly registered for online access and are conducting large amounts of activity compared to previous account activity.
ORT009	Flow Through Account Transactions	Identifies where, a customer is using one or more accounts to circulate funds. Circulation of funds is a scenario where funds will be deposited, and then rapidly withdrawn from one or more accounts.
ORT010	New IP Address Login with Large Transactions	Identifies customers that login from a new IP address then conduct activity over a certain threshold.
ORT011	New IP Address Login with Personal Information Change	Identifies customers that login from a new IP address and then change personal information on the account (address, email, phone, etc.)
ORT012	Multiple Failed Logins Followed by Large Transactions	Identifies customers that have multiple failed logins before a successful one and then conduct a large transaction.
ORT013	New Bill Payment Setup with Excessive Volume of Payments	Identifies customers where a new bill payment vendor is setup followed by excessive payments to that vendor.
ORT014	New Bill Payment Setup with Excessive Value of Payments	Identifies customers where a new bill payment vendor is setup followed by a large payment to that vendor.
ORT015	New Bill Payment Setup from International Location	Identifies customers where a new bill payment vendor is setup from a foreign location.
ORT016	Dormant to Active Online Account Status	Identifies customers that have not logged in for a specified number of months, and then have activity above specified thresholds.
ORT017	High Velocity ATO EMT Rule	Identifies when a large number of low dollar EMTs are being sent out within a set period of days.
ORT018	High-Risk Vendor Rule	Identifies high risk vendors and determines if transactions involve high risk bill payment activities.
ORT019	Extended EMT response validation rule	The rule will examine and approve all transactions passing through this rule and have the ability to create cases for

		investigation. Decisioning relies on a transaction's activity code and notification handle. This rule will not have the ability to decline transactions, only approve them.
ORT020	Known Mobile Device	Identifies if transactions were completed from a known mobile device and the device had a total session time of 30 minutes or greater. If not, depending on activity type, an event can be generated to review.
ORT021	Mobile Device Usage Rule	Identifies number of unique members using a given mobile device and can generate event on specified account activities above a certain threshold.
ORT022	High Risk Activity Codes	Identifies specific transaction types deemed to be "high risk" and generate events on those transactions
ORT023	Modified e-Transfers	Identifies if an eTransfer transaction was completed following a certain sequence of activity codes that are deemed high risk in combination.
ORT024	Known Bill Payees	Identify bill payees that have been determined to be low risk and transactions can be approved without further review.
ORT025	EMT Account Take Over	Identify electronic money transfer (EMT) transactions whose accounts meet account takeover risk factor.
ORT026	Credit Card Bill Payments with High-Risk Properties	Identifies high risk credit card bill payments.
ORT027	New Bill Payment Beneficiary After Login from New IP Address	Identifies a new bill payment beneficiary appearing after a login from a new IP Address.
ORT028	Online IP Blacklist Rule	Identifies online transactions initiated from specified blacklisted IP Addresses.
ORT029	High-Risk E-transfers	Identifies high risk E-Transfers based on transaction amount, recent historical transaction activity, location and other risk factors.
ORT030	High-Risk Outbound Specified Transaction Party Rule	The intent of this rule is to detect high risk outbound transactions to a specific party (e.g. MoneyMover, or TransferWise) based on behavior exclusive of IP inconsistency.
ORT031	Money Request E-Transfer Rule	Evaluate fulfilled money request e-transfers and decision approval based on transaction amount, recent historical transaction activity, location and other risk factors.
ORT032	New Same Ip E-Transfer Rule	Identify E-transfers when they exceed an amount threshold and are greater than the average E-transfer value of a set number of

		days. This rule will apply if the E-transfers are coming from the same IP address.
ORT033	Bill Beneficiary Rule	Identify when a new bill beneficiary has been added to an account after a bill payment is made.

3. Tuple Message Data Model

The following table shows the tuple message data model used for monitoring online banking and financial platform transactions.

Field	Field Description	Example	Priority*
TRANSACTION_ID	Unique Transaction Identifier	000123456789	S
DATETIME	Date and Time of Transaction	2021-01-29 21:13:32.020	S
SESSIONID	Unique Session Identifier	1sdf3554-f235-24c5-24c2-85s3430a232	S
USERID	Unique User Identifier	3435332	S
CUSTNO	Unique Customer Identifier	3435332	S
CUSTBRANCH	Branch Customer belongs to	JBank	S
CUSTBENEFIT	Customer Benefit Type	REGULAR	S
STAFFID	Unique Staff Identifier	1234	E
ACTIVITYCODE	Type of Transaction	14705	S
UICODE	UI Type Code	2	S
MOBILEDEVICECODE	Mobile Device Type Code	2	S
MOBILEDEVICEMACID	Mobile Device MAC ID	825843B8-546F-5365-6465-F35436D3543	S
CLIENTIP	Client IP Address	65.19.37.116	S
ACCOUNTID1	Primary Account Identifier	1999063543584	S
ACCOUNTNAME1	Primary Account Type	Line of Credit	S
ACCOUNTID2	Secondary Account Identifier	100006587683	E
ACCOUNTNAME2	Secondary Account Type	66323435 – Line of Credit -1	E
VENDORNAME	Vendor Name	Amazon	E
VENDORACCT	Vendor Account	1222234455	E
AMOUNT	Transaction Amount	70.00	S
PRODUCTID	Product Type Identifier	123	S
ERRORCODE	Error Code	20020	E
ERRORMESSAGE	Error Description	Customer not setup for Online Banking	E
HTTP_CS_URI_STEM	HTTP CS URI STEM	Default.htm	E

HTTP_CS_URI_QUERY	HTTP CS URI QUERY	?type=accept	E
HTTP_CS_HOST	HTTP CS HOST	http://www.bank.com	E
HTTP_USER_AGENT	HTTP USER AGENT	iphone12	E
HTTP_CS_REFRRER	HTTP CS REFERRER	http://www.bank.com	E
HTTP_LOCAL_TIME	HTTP LOCAL TIME	Sun, 01 DEC 2020 08:49:37 GMT	E
HTTP_BEGIN_REQUEST_UTC	HTTP BEGIN REQUEST UTC	Sun, 01 DEC 2020 08:49:37 GMT	E
SCHEMA_NAME	Schema Name	ONLINE	S
GATEWAY_ID	Gateway ID	/172.25.54.63:35434	S
CREATED_DATE	Date the Transaction was created	2021-01-09 17:00:42.327	S
RESPONSE_CODE	Response given to the transaction	1	S
participantUserId	Unique Participant Identifier	6854684318	S
productCode	Product code	0	S
transferType	Transfer Type Code	2	S
contactId	Unique Contact Identifier	SDfaweSXCER	S
currencyCode	Transaction Currency Code	CAD	S
emt_api_amount	EMT API Transaction Amount	70	S
originatingCurrencyCode	Originating Currency Code	CAD	E
originatingAmount	Originating Amount	70	E
expiryDate	Expiration date of Transaction	2021-01-09 17:00:42.327	E
senderMemo	Sender Memo	“For Rent”	E
participantReferenceNumber	Participant Reference Number	12222454	E
participantTransactionDate	Participant Transaction Date (will default to earliest date if not known)	1900-01-01 00:00:00.000	E
contactNameAliasName	Full Name of Contact	Nancy Richardson	S
firstName	First Name of Contact	Nancy	E
middleName	Middle Name of Contact	Emilia	E
lastName	Last Name of Contact	Richardson	E
companyName	Full Name of Company	East India Trading	E

tradeName	Trade Name of Company	EITC	E
notificationHandleType	Type of contact information (ex. 0 = “email address”)	0	S
notificationHandle	Contact information	myname@gmail.com	S
active	Active account (1= yes, 0 =no)	1	E
address1	Address Line 1	10 First Road	E
address2	Address Line 2	Unit 134	E
city	City	Montreal	E
province	Province	Quebec	E
postalCode	Postal Code	G1A 0A2	E
country	Country	Canada	E
groupId	Group ID	15445	E
requestReferenceNumber	Reference Number of the Request	2234234	E
directDepositReferenceNumber	Direct Deposit Reference Number	CSDF656736SDF	E
senderAccountIdentifier	Account Identifier of Sender	10000444444	E
fiAccountId	Financial Account Identifier	10087687676874	E
accountHolderName	Full Name of Account Holder	Frederick Lutz	S
bankAccounttype	Bank Account Type (code)	1	S
authenticationType	Type of Authentication (code)	2	S
securityQuestion	Security Question	Mother’s Maiden Name	E
customerCardNumber	Customer Card Number	5631386	S
accountCreationDate	Account Creation Date (will default to earliest date if not known)	1900-01-01 00:00:00.000	E
customerDeviceFingerprint	Customer Device Unique Fingerprint		E
authenticationMethod	Authentication Method	1	E
directDepositHandle	Direct Deposit Identifier	1232342342	E
accountNumber	Account Number	10000323412123	S
transferReferenceNumber	Transfer Reference Number	SNLnclsiHS	S
fraudScore	Fraud Score	High Risk	E
fraudReason	Fraud Reason	Fraud Watchlist	E

beginTransactionId	Transaction Start Identifier	SDFfdsadNSDF	E
recipientMemo	Recipient Memo	Approved	E
Flex1	Flex 1	AAA	E
Flex2	Flex 2	BBB	E
Flex3	Flex 3	CCC	E
OLB_ACTION	Online Banking Action Step	null	E

It should be noted that "S" in the table above represents a field required for standard, or base monitoring functionality, while "E" indicates a field required for enhanced monitoring functionality.

4. Resultant Tuple Structure

Available data for monitoring is mapped to a standard EnScreen ESP tuple as shown in the example below:


```
TUPLE_START=ONLINE{TRANSACTION_ID="234234205829342093482930"|DateTime="2020-12-
01 06:25:10:177"|SessionId="87c34aa4-c951-4dc2-989c-
c623c5343342"|UserID="020120336"|CustNo="500650352"|CustBranch="ontario"|CustBe
nefit="Individual"|StaffId="252252"|ActivityCode="12323"|UICode="1"|MobileDevic
eCode="1"|MobileDeviceMACId="64545A1-333E-333D-b3a1-
362541B89852"|ClientIP="123.123.123.12"|AccountId1="3266565623"|AccountName1="L
ine of
Credit"|AccountId2="1232123"|AccountName2="Demand"|VendorName="Amazon"|VendorAc
ct="356465203"|Amount="70"|ProductId="123123"|ErrorCode="11"|ErrorMessage="Not
Setup for Online
Banking"|HTTP_CS_URI_STEM="Transaction.htm"|HTTP_CS_URI_QUERY="?type=accept"|HT
TP_CS_HOST="http://www.bank.com"|HTTP_USER_AGENT="iPhone9"|HTTP_CS_REFRRER="htt
p://www.bank.com"|HTTP_LOCAL_TIME="Sun, 01 DEC 2020 08:49:37
GMT"|HTTP_BEGIN_REQUEST_UTC="Sun, 01 DEC 2020 08:49:37
GMT"|participantUserId="2234234234"|productCode="0"|transferType="2"|contactId=
"SDfaweSXCER"|currencyCode="CAD"|emt_api_amount="70"|originatingCurrencyCode="C
AD"|originatingAmount="70"|expiryDate="2020-12-01"|senderMemo="For
Paper"|participantReferenceNumber="51651656563"|participantTransactionDate="202
0-12-01"|contactNameAliasName="Jeff
B."|firstName="Jeff"|middleName="R"|lastName="Bezos"|companyName="Amazon"|trade
Name="AMZN"|notificationHandleType="0"|notificationHandle="myname@me.com"|activ
e="1"|address1="10 First Rd"|address2="Unit
2"|city="Montreal"|province="QC"|postalCode="G1A
0A2"|country="CA"|groupId="15445"|requestReferenceNumber="f23423423432"|directD
epositReferenceNumber="64543535345"|senderAccountIdentifier="23423455"|fiAccoun
tId="655464565"|accountHolderName="Jeff
Bezos"|bankAccounttype="Demand"|authenticationType="1"|securityQuestion="Mother
's Maiden
Name"|customerCardNumber="235523698574125486"|accountCreationDate="2012-02-
15"|customerDeviceFingerprint=""|authenticationMethod="1"|directDepositHandle="
321565132"|accountNumber="4234234234"|transferReferenceNumber="234253442"|fraud
Score="100"|fraudReason="Fraud
```

```
Watchlist"|beginTransactionId="32423423"|recipientMemo="Approved"|Flex1="XXX"|F
lex2="YYY"|Flex3="ZZZ"|}TUPLE_END=ONLINE
```

Mandatory fields for monitoring within the above tuple structure are as follows:

```
TRANSACTION_ID
DateTime
ActivityCode
ClientIP
Amount
HTTP_CS_HOST
```

5. Submission of Tuples and Responses from NOD-RT

Tuples may be submitted to NOD-RT for processing in two separate modes:

1. Asynchronous submit/inquire; or
2. Synchronous

5.1 Responses in Synchronous Mode

When submitting data, and receiving responses from NOD-RT on the same session, the following tuple will be passed back in the output stream:

```
TUPLE_START=ONLINE{Transaction_id="0200541599"|RESPONSE_CODE="1"}TUPLE_END=ONLI
NE'
```

This tuple associates with the inbound request based on the Transaction_ID value, and returns the RESPONSE_CODE value to indicate 1 for ‘Allow’ or 2 for ‘Block’.

5.2 Responses in Asynchronous Mode

When submitting data and receiving responses in two separate sessions, inbound tuples will be structured identically as with those submitted for synchronous processing. However, in an asynchronous implementation, a separate status check message is used to retrieve the results of processing. The status check tuple structure is discussed in the following sections.

5.2.1 Request Status Check Message

The status check request message is sent to NOD-RT with a transaction ID value for status check the request, as well as a Check_Transaction_ID value to indicate the transaction ID for which status is being requested. The tuple structure appears as follows:

```
TUPLE_START=STATUS_CHECK{TRANSACTION_ID="1585401378191"|CHECK_TRANSACTION_ID="2
003271754 "}TUPLE_END=STATUS_CHECK
```

5.2.2 Response Status Check Message

The status check response message indicates the submitted Transaction_ID value along with the response code for the input Check_Transaction_ID value submitted in the request.

```
TUPLE_START=STATUS_CHECK{TRANSACTION_ID="1585401378191"|RESPONSE_CODE="2"}TUPLE
_END=STATUS_CHECK
```

Response codes from NOD-RT status check message are as follows:

1 = Allow
0 = Block
2 = Pending (Status-Check Only)
3 = Transaction not found (Status-Check Only)