Integration Guide for EnScreen ESP Real-Time Fraud Monitoring Schemes for Global FSI Card/Payment Fraud

Proprietary and Confidential

Navaera Sciences, LLC

February 1, 2021

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 payments monitoring. As a general standard, the data/tuple structures for payment monitoring follow the IS0-8583 Financial Transaction message standard. In this document, we will overview typically implemented fraud schemes, review typical data population, and also review the structure of a typical key-value paid 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 card or payment transactions for fraudulent activity. Card or payment 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 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.

Global filters are designed to remove any transactions known to not represent substantive risk of fraud. Examples of global filters may include filtering card transactions domestic chip/pin transactions to focus monitoring on online, or magnetic stripe transactions only. Global filters can be designed easily based on business objectives, and can be modified at any time.

2.2 Transaction Level Rules

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

Scheme Code	Scheme Short Description	Scheme Analysis Description
CRT101	Merchant Terminal Blacklist	Identifies customers who are conducting activity from a merchant terminal that is blacklisted.

CRT102	Compromised Terminal	Identifies customers where transactions are being conducted at a potentially compromised terminal.
CRT103	Transactions from Multiple Countries	Identifies customers who are conducting transactions from multiple countries within a short period of time or a period of time that would not match the travel time between those countries.
CRT104	Transactions from High Risk Jurisdictions	Identifies customers who are conducting transactions from high-risk jurisdictions.
CRT105	Total Card Spend	Identifies customers who are conducting activity over a predefined threshold.
CRT106	Total Country Spend	Identifies transactions from countries where there is an abnormal amount of activity.
CRT107	High Value Foreign Card Transactions	Identifies customers who are conducting large transactions from a foreign country.
CRT108	High Velocity Foreign Card Transactions	Identifies customers who are conducting an excessive amount of card transactions from a foreign country.
CRT109	Low Dollar Approval	Identifies any transactions that are under a low dollar threshold amount and automatically approves them.
CRT110	High Spend Debit Card Rule	Identifies high dollar/velocity transaction activities on Debit Cards and generates events if the total volume or value of debit card transactions over a set period exceeds the specified threshold.
CRT111	US Merchant Rule	Identifies if a transaction occurred in the United States within a specific geographic region and at a specified merchant and if it exceeds a threshold amount; if so, it will decline the transaction.
CRT112	Geo-Fence: Total Portfolio Spend	Identifies cases where the total portfolio spend across all members exceeds a specified amount in a particular country and declines the transaction(s).
CRT113	Geo-Fence: Total Portfolio Spend US State	Identifies cases where the total portfolio spend across all members exceeds a specified amount in a particular US State and declines the transaction(s).

CRT114	Geo-Fence: Individual Spend	Identifies a customer that exceeds a set amount in total (ex. $250) in a 24-hour period in an individual country outside of Canada and the US and declines the transaction(s).
CRT115	Foreign Transaction Time Delay Rule	Identifies overseas transactions or transactions in a foreign country that follow a transaction in Canada within a specified short amount of time and if it is below the time threshold, the foreign transaction will be declined.
CRT116	Multiple Plastics at Non-Canadian ATMs	Identify card skimming at specific locations based on the value and volume of activity. This rule uses the B043CardAcceptorNameLoc field to identify countries outside of Canada.
CRT117	Inbound Specified Source AMBPOS Rule	Identifies inbound transactions from a specific source (e.g. MoneyMover, or TransferWise) that may carry fraud risk and declines them. The rule will identify cases for decline based on transaction amount threshold, whether the member is on a Safe List, the individual's portfolio spend over a set lookback period, the total amount of inbound transactions within a set time period, and whether the transaction was completed overnight.

3. Tuple Message Data Model

The following table shows the tuple message data model used for monitoring payment transactions. As indicated earlier, the message structure is based on ISO 8583:1987, though additional fields have been added to improve processing performance, or to provide additional detail to a reviewer if needed.

For ISO-8583 fields, the first four characters of the field name indicate the ISO 8583:1987 bit sequence. For example, B002 indicates bit 2 which contains the PAN, while B005 corresponds to bit 5, and indicates the settlement amount.

Field	Field Description	Example	Priority*
TRANSACTION_ID	Unique Transaction Identifier	0200504466	S
HEADMSGTYPE	Heading Message Type	0200	S
B002PAN	Primary Account Number	132543547313513133	S
B003PROCESSING	Processing Code	002000	S
B004TXNAMT	Transaction Amount	50.00	S
B005SETAMT	Settlement Amount	000000000000	S
B007TXDATETIME	Transaction Date & Time	2021-01-09 17:00:42.327	S
B009SETCONVRATE	Conversion rate, settlement	00000000	S
B011SYSTRACE	System trace audit number (STAN)	802153	S
B012LOCTXNTIME	Local transaction time (hhmmss)	051712	S
B013LOCTXNDATE	Local transaction date (MMDD)	12082020	S

B014EXPDATE	Card Expiration Date	202610	S
B016CONVDATE	Date of conversion (defaults to earliest date if no value is found)	01011900	S
B018MERCHANT	Merchant Code	5540	S
B022POSENTRYMODE	Point of Service Entry Mode	051	S
B023CARDSEQ	Application PAN sequence number	000	S
B025POSCONDITION	Point of Service Condition Code	01	S
B026POSCAPCODE	Point of Service Capture Code	12	S
B032ACQINSTID	Acquiring institution identification code	101010010101	S
B033FWDINSTID	Forwarding institution identification code	105353123530	S
B035TRACK2	Track 2 data	353513513513513532= 32513213213558311212	S
B037RETRIEVALREFERENCE	Retrieval reference number	000000074532	S
B038AUTHIDRESP	Authorization identification response	092132	S
B039RESPONSE	Response code	00	S

B040RESTRICTIONCODE	Service Restriction Code	220	S
B041CARDACCEPTORTERMID	Card Acceptor Terminal Identification	54351320	S
B042CARDACCEPTORID	Card Acceptor Identification Code	453130000000000	S
B043CARDACCEPTORNAMELOC	Card acceptor name/location	BANK OF MONTREAL TORONTO ONCA	S
B049TXNCURRENCY	Transaction Currency Code	124	S
B050SETCURRENCY	Settlement Currency Code	000	S
B056REASONCODE	Reason Code	000	E
B057LIFECYCLECODE	Lifecycle Code	000	E
B074CREDITSNUMBER	Number of Credits	11	E
B075CREDITSREVERSAL	Credits, reversal number	12	E
B076DEBITSNUMBER	Number of debits	11	E
B077DEBITSREVERSAL	Debits, reversal number	12	E
B102ACCTID1	Account identification 1	65846843643846384	S
B103ACCTID2	Account identification 2	00	S
B123POSDATA	Point of Service Data	257A35435435435432	E
B127TERMINALOWNER	Terminal Owner	00BANKNAME	E
B127POSGEOGRAPHIC	Point of Sale Geographic	23153L3N 4D5 231	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=CARD{Transaction_id="A-233445-
20201205120000001"|HeadMsgType="10011"|B002PAN="132496851342576985"|B003Process
ing="135842"|B004TxnAmt="000000102200"|B005SetAmt="000000102200"|B007TxDateTime
="1220051200"|B009SetConvRate="00000000"|B011SysTrace="254259"|B012LocTxnTime="
120000"|B013LocTxnDate="12052020"|B014ExpDate="201206"|B016ConvDate="20123548"|
B018Merchant="4253"|B022POSEntryMode="081"|B023CardSeq="000"|B025POSCondition="
00"|B026POSCapCode="12"|B032AcqInstId="657895345628"|B033FwdInstId="10345298752
3"|B035Track2="552556633=566523156
6"|B037RetrievalReference="000009652438"|B038AuthIdResp=" adasdff3
"|B039Response="23"|B040RestrictionCode="222"|B041CardAcceptorTermId="63425875"
|B042CardAcceptorId="0040208966551"|B043CardAcceptorNameLoc="AMAZON 02423
TORONTO
ONCA"|B049TxnCurrency="124"|B050SetCurrency="000"|B056ReasonCode="0524520"|B057
LifeCycleCode="000"|B074CreditsNumber="12"|B075CreditsReversal="14"|B076DebitsN
umber="13"|B077DebitsReversal="11"|B102AcctId1="3213253213553"|B103AcctId2="00"
|B123POSData="023A95245760352121"|""|""}TUPLE_END=CARD
```

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

```
Transaction_id
HeadMsgType
B002PAN
B004TxnAmt
B005SetAmt
B007TxDateTime
B009SetConvRate
B012LocTxnTime
B013LocTxnDate
```

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=CARD{Transaction_id="0200541599"|RESPONSE_CODE="1"}TUPLE_END=CARD'
```

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)