TECHNICAL PAPER

SAS® Fraud Management Customer Contact Enablement and Automation

Last update: October 2020

Contents

Relevant Products and Releases....................2

Abstract....................3

Overview....................3

- The Interactive Voice and Response System Interface.................... 3
- The Enterprise Case Management Interface.................... 6
- The Automation Interface.................... 8

Customer Contact Process Flows via the IVRS and ECM Interfaces....................11

- Confirmed No Risk Scenario.................... 11
- Confirmed Risk Scenario.................... 11
- Unconfirmed Risk Scenario.................... 12
- Error Handling.................... 13

Customer Contact Process Flows via the Automation Interface....................13

- Confirmed No Risk Scenario.................... 13
- Confirmed Risk Scenario.................... 14
- Unconfirmed Risk Scenario.................... 15

References....................17

Relevant Products and Releases

- SAS® Fraud Management 5

Abstract

Speed is a key aspect in fraud detection and prevention. This includes the speed of contacting your customers and taking preventative actions. Read this technical paper to find out how SAS® Fraud Management can empower you to reach the speed that you need to stay ahead of fraud risks.

Overview

SAS Fraud Management is best known for its powerful advanced analytics capabilities that can do the following:

- Fight enterprise-wide fraud on a single platform.
- Score 100% of transactions and events in real time.

Besides these capabilities, SAS Fraud Management can also integrate with other systems to automate critical actions. This is often referred to as business process management, and these tasks would otherwise be performed manually by fraud analysts. An example of this would be when you contact a customer to verify whether a transaction is genuine, and you immediately take the necessary actions to minimize either fraud losses or customer inconvenience.

This document describes how you can achieve optimal performance using the following features that are available as part of core SAS Fraud Management:

- Interactive Voice and Response System (IVRS) interface (also known as the Customer Contact System or CCS interface)
- Enterprise Case Management Interface (ECMI)
- Automation interface
- Real-time response from rules

These features enable you to automatically and quickly contact your customers via any channel (for example, IVRS, SMS text message, PUSH, email, or voice mail) quickly once suspicious activity is detected. Subsequently, the ECMI and the automation interface enable you to automatically trigger downstream alert actions based on the result of the customer contact attempt whether it was successful or not, and whether the customer confirmed the transactions to be fraud or genuine. The automation interface enables you to do both and more through the REST API. The following sections describe each of these interfaces in greater detail.

The Interactive Voice and Response System Interface

The IVRS interface provides a much wider capability to reach your customers through any channel. Through this interface, your preferred CCS calls a set of web services (via SOAP) to perform the following operations:

- Retrieve alert information from SAS Fraud Management, which can include customer and transaction data.
- Update alerts as contact attempts are made.
- Save changes to alerts based on the result of the contact attempts and the customer response (if the attempts are successful).

This interface and the definition of these web service operations (commonly known as WSDL) are readily available once SAS Fraud Management is installed and the SAS Alert Management System (SAMS) is used. To find out more about how these web services work, see *SAS Fraud Management: Message Specification*. View the Resources section of this paper to access SAS Fraud Management documentation.

To start using this interface, complete these steps:

1. Log on to SAS Fraud Management as a System Administrator or Sr Manager, or with any role that has the following privileges:
    a. Add/Delete/Modify Strategies and Queues
    b. Add/Delete/Modify Users
    c. General Manager Access
    d. Modify Preferences
    e. Modify System Properties
    f. View Preferences
    g. View Strategies and Queues
    h. View System Properties
    i. View User Roles
    j. View Users
2. Select the **Users** tab.
3. Click **New User** and create a user for the customer contact system. Assign it to the role of an Analyst. Make sure that the user has the following credentials:
    a. Assigned to a team
    b. Access to the alert types and multi-organizational nodes to which it will send notifications
    c. Assigned to the business units that contain the strategies and queues from which it will retrieve alerts
4. Once you create the user, run `Job 3` as the `sasomr` user on the SAS Fraud Management batch server. This job is used to add newly created users to the SAS Metadata Repository, which is required before the user can log on. For Instructions about how to run `Job 3`, see *SAS Fraud Management: System Administrator's Guide* in the section named "Load Users in SAS Metadata Repository (Job 3)." View the Resources section of this paper to access SAS Fraud Management documentation.
5. Select the **Strategies** tab.
6. Assign the customer contact system user to the strategy (or strategies) from which it will retrieve and service alerts.
7. Review the strategy and queue priorities. These priorities determine the order in which alerts are serviced and affect the order in which customers are contacted. For more information about prioritizing strategies and queues, see the chapter about the **Strategies** tab in *SAS Fraud Management: Manager's Workbench User's Guide*. View the Resources section of this paper to access SAS Fraud Management documentation.
8. Review the queue's **Call Result Settings** because they determine the following:
    a. The call results that can be applied to alerts (for example, **Save Pending with Block**, **Verified Activity**, **Reroute**, and so on)

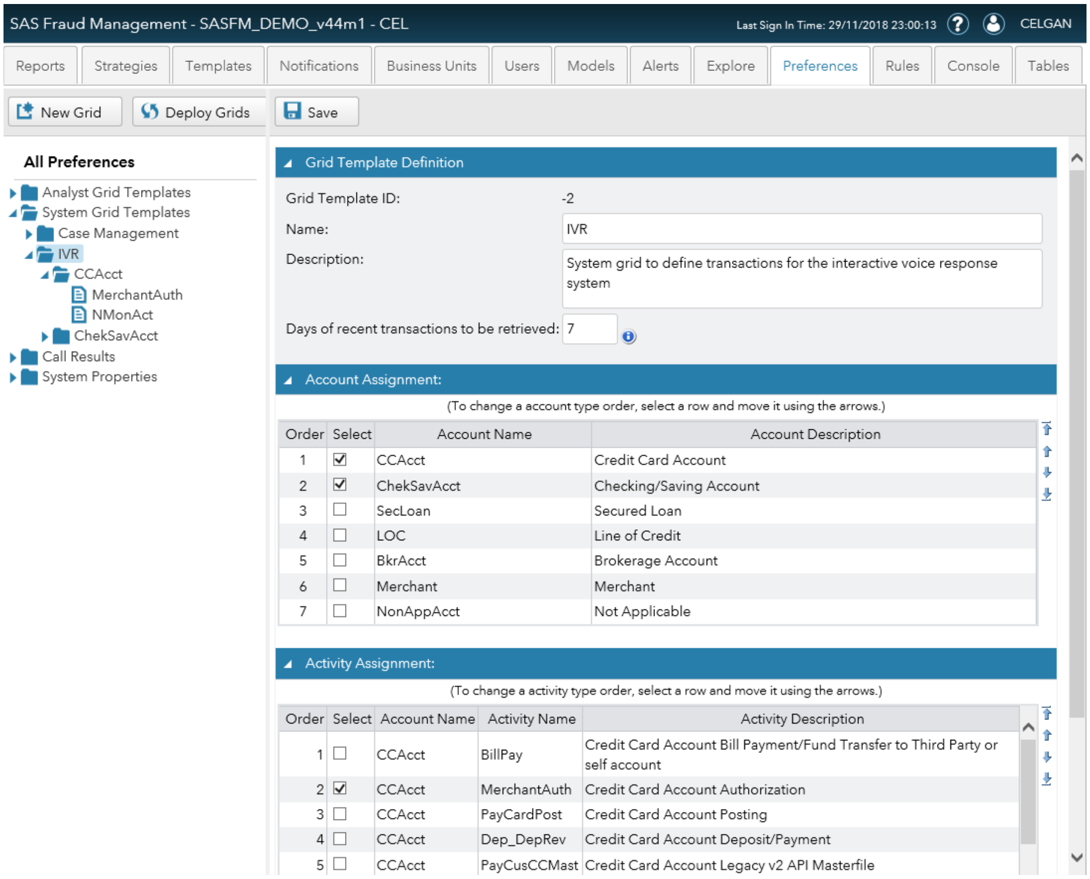
b. The actions that can be applied to alerts (for example, what blocks can be placed) for each call result

If the customer contact system attempts to apply a call result or a block code that has not been configured for the strategies and queues that are assigned to it, then an error message is sent.

9. Select the **Preferences** tab. Expand the **System Grid Templates** folder and select the **IVR** system grid. Check the following:

   a. Make sure that all the account types and activity types that customer notifications are sent to are selected.

   __Figure 1.__ The IVR system grid



Grid Template ID: -2

Name: IVR

Description: System grid to define transactions for the interactive voice response system

Days of recent transactions to be retrieved: 7

(To change a account type order, select a row and move it using the arrows.)

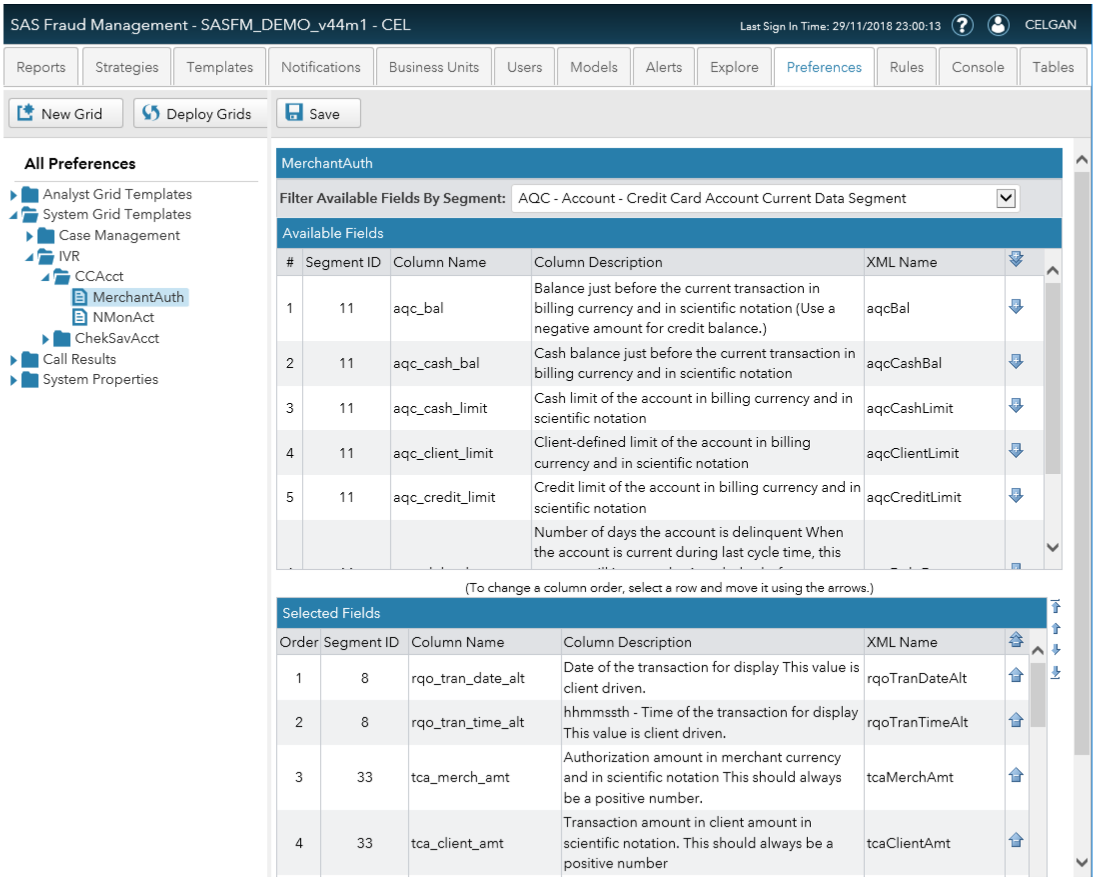
Order	Select	Account Name	Account Description
1	☑	CCAcct	Credit Card Account
2	☑	ChekSavAcct	Checking/Saving Account
3	☐	SecLoan	Secured Loan
4	☐	LOC	Line of Credit
5	☐	BkrAcct	Brokerage Account
6	☐	Merchant	Merchant
7	☐	NonAppAcct	Not Applicable

(To change a activity type order, select a row and move it using the arrows.)

Order	Select	Account Name	Activity Name	Activity Description
1	☐	CCAcct	BillPay	Credit Card Account Bill Payment/Fund Transfer to Third Party or self account
2	☑	CCAcct	MerchantAuth	Credit Card Account Authorization
3	☐	CCAcct	PayCardPost	Credit Card Account Posting
4	☐	CCAcct	Dep_DepRev	Credit Card Account Deposit/Payment
5	☐	CCAcct	PayCusCCMast	Credit Card Account Legacy v2 API Masterfile

   b. For each activity type under an account type, make sure that all the required fields for the customer notifications are found in the **Grid Template**. Only the fields that are found in this grid are included when the customer contact system retrieves the alert information.

Figure 2. *Merchant authorization fields for credit card accounts in the IVR system*



SAS Fraud Management - SASFM_DEMO_v44m1 - CEL

Last Sign In Time: 29/11/2018 23:00:13 CELGAN

MerchantAuth

Filter Available Fields By Segment: AQC - Account - Credit Card Account Current Data Segment

Available Fields

#	Segment ID	Column Name	Column Description	XML Name	⬇
1	11	aqc_bal	Balance just before the current transaction in billing currency and in scientific notation (Use a negative amount for credit balance.)	aqcBal	⬇
2	11	aqc_cash_bal	Cash balance just before the current transaction in billing currency and in scientific notation	aqcCashBal	⬇
3	11	aqc_cash_limit	Cash limit of the account in billing currency and in scientific notation	aqcCashLimit	⬇
4	11	aqc_client_limit	Client-defined limit of the account in billing currency and in scientific notation	aqcClientLimit	⬇
5	11	aqc_credit_limit	Credit limit of the account in billing currency and in scientific notation	aqcCreditLimit	⬇
			Number of days the account is delinquent When the account is current during last cycle time, this		

(To change a column order, select a row and move it using the arrows.)

Selected Fields

Order	Segment ID	Column Name	Column Description	XML Name	⬆
1	8	rqo_tran_date_alt	Date of the transaction for display This value is client driven.	rqoTranDateAlt	⬆
2	8	rqo_tran_time_alt	hhmmssth - Time of the transaction for display This value is client driven.	rqoTranTimeAlt	⬆
3	33	tca_merch_amt	Authorization amount in merchant currency and in scientific notation This should always be a positive number.	tcaMerchAmt	⬆
4	33	tca_client_amt	Transaction amount in client amount in scientific notation. This should always be a positive number	tcaClientAmt	⬆

10. Once you configured all the fields for each account and activity type in the **IVR** system grid, click **Save**. These changes take effect within one hour automatically. If the changes need to take effect as soon as possible, click **Deploy Grids**.

    Note: Clicking **Deploy Grids** deploys all the grids that have been configured in the **Preferences** tab, not just the **IVR** grid.

    For more information about how to perform each of these tasks, see *SAS Fraud Management: Manager's Workbench User Guide*. View the Resources section of this paper to access SAS Fraud Management documentation.

11. Expand the **System Properties** folder. Select **IVR**. The last five properties in the list are IVR-related properties. These properties contain default values. Review these values to see whether you need to change them. If you make changes, click **Save** so that your changes take effect. For more information about the IVR properties, see the section named "Configuring the Interactive Voice and Response System" in *SAS Fraud Management: Message Specification*. View the Resources section of this paper to access SAS Fraud Management documentation.

The Enterprise Case Management Interface

The Enterprise Case Management (ECM) interface is designed for SAS Fraud Management to integrate with a case management system where longer-term investigations can occur. Its event-based mechanism sends alert information from SAS Fraud Management to a data consumer in the form of an XML message. By default, the message contains information about the alert and the alerting entity, as well as the associated parent (optional) and contact entities (for example, account, card, payment, and so on). If configured, it can also include the actions to be taken on the alerting entity, as well as transaction data for those transactions where the **CF** check box was selected. This means that when an alert is serviced and checked back in (that is, an event), it can be leveraged to trigger actions such as blocking and unblocking cards, holding and releasing payments, and leaving notes on the customer profile.

Like the IVRS Interface, ECMI is readily available once SAS Fraud Management is installed, and the SAS Alert Management System is used. However, unlike the IVRS interface, a middleware broker or end-point consumer (such as the SAS® Business Orchestration Services) must listen for the ECMI messages and process them upon receipt. Because SAS Fraud Management does not favor a specific vendor, ECMI uses a generic XML message over MQ that can be consumed by any system, and the data within the ECMI message might need transformation. For more information about this interface, see the chapter named “Case Management Integration” *in SAS Fraud Management: Message Specification*. View the Resources section of this paper to access SAS Fraud Management documentation.

Besides competing the steps in the chapter “Case Management Integration” in *SAS Fraud Management: Message Specification*, be sure to complete the following steps before using the ECMI:

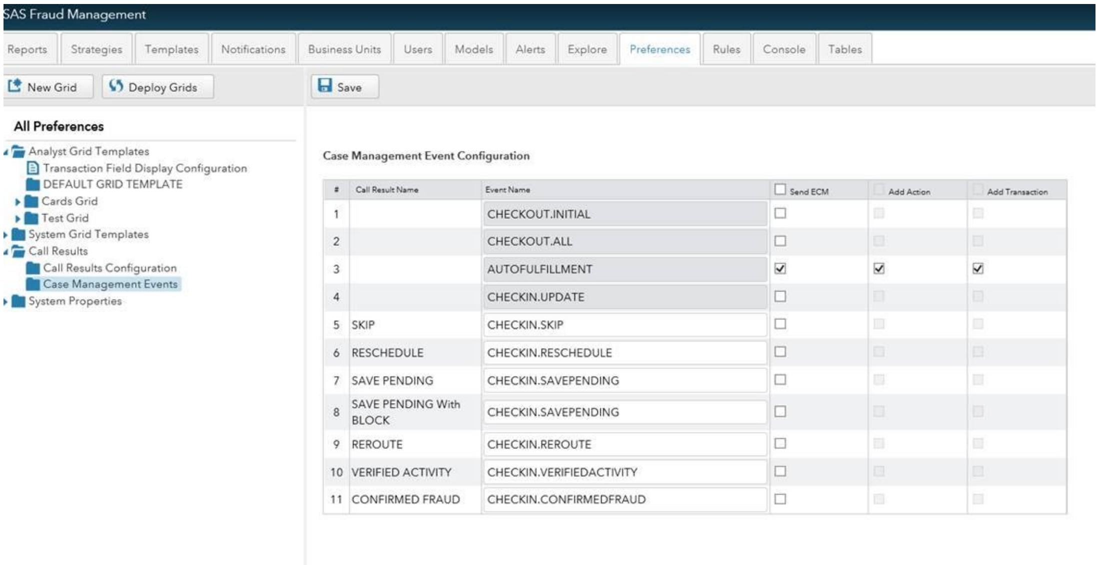
1. Log on to SAS Fraud Management as a System Administrator or Senior Manager, or any role that has the following privileges:
   a. General Manager Access
   b. Modify Preferences
   c. Modify System Properties
   d. View Preferences
   e. View System Properties
2. Select the **Preferences** tab. Expand the **System Grid Templates** folder. Select **Case Management**. Check the following:
   a. Make sure that all the account types and activity types that the ECMI XML messages will be sent to are selected.
   b. For each activity type under an account type, make sure that all the required fields for the customer notifications are found in the Grid Template. Only the fields that are found in this grid are included when the customer contact system retrieves the alert Information.
3. Once you configure all the fields for each account and activity type in the **Case Management** system grid, click **Save**. These changes take effect within one hour automatically. If the changes need to take effect as soon as possible, click **Deploy Grids**.

   Note: Clicking **Deploy Grids** deploys all the grids that have been configured in the **Preferences** tab, not just the **Case Management** grid.
4. Configure the events that trigger an ECMI message to be sent. Expand the Call Results folder. **Select Case Management Events**.

   The **Case Management Event Configuration** table lists the call results that are configured in the system and their corresponding event names.

5. Select the check box in the **Send ECM** column for each call result that you want to send an ECMI message to. That means that every time an alert is saved with that call result, an ECMI message is sent.

Figure 3. *The Case Management Event Configuration table*



Case Management Event Configuration

#	Call Result Name	Event Name	☐ Send ECM	☐ Add Action	☐ Add Transaction
1		CHECKOUT.INITIAL	☐	☐	☐
2		CHECKOUT.ALL	☐	☐	☐
3		AUTOFULFILLMENT	☑	☑	☑
4		CHECKIN.UPDATE	☐	☐	☐
5	SKIP	CHECKIN.SKIP	☐	☐	☐
6	RESCHEDULE	CHECKIN.RESCHEDULE	☐	☐	☐
7	SAVE PENDING	CHECKIN.SAVEPENDING	☐	☐	☐
8	SAVE PENDING With BLOCK	CHECKIN.SAVEPENDING	☐	☐	☐
9	REROUTE	CHECKIN.REROUTE	☐	☐	☐
10	VERIFIED ACTIVITY	CHECKIN.VERIFIEDACTIVITY	☐	☐	☐
11	CONFIRMED FRAUD	CHECKIN.CONFIRMEDFRAUD	☐	☐	☐

6. If you want to include data about the alert actions in the ECMI message (for example, block codes and whether they are added or removed), then select the check box in the **Add Action** column for each call result that you would like this information to be included.

7. If you want to send transaction data in the ECMI message, then select the check box in the **Add Transaction** column for each call result that you would like this information to be included.

   Note: For the first two events in the **Case Management Event Configuration** table (CHECKOUT.INITIAL and CHECKOUT.ALL) and any auto-fulfillment events, the transaction data that is included is based on the transaction that triggered the alert. For the rest of the events, it includes the transactions that were marked as confirmed fraud.

8. Click **Save**.

For more information about how to perform each of these tasks, see *SAS Fraud Management: Manager's Workbench User Guide*. View the Resources section of this paper to access SAS Fraud Management documentation.

The Automation Interface

The automation interface enables you to automatically trigger many actions that a fraud analyst can do via a REST API. This includes sending customer notifications, updating alerts, marking transactions as fraud, and creating manual alerts (that is, if there was no alert generated for a suspicious transaction, then one can be created through this interface).

Broadly, they are classified under alert actions, analyst actions, and transaction actions. Here is the list of actions under each of the categories:

Alert Actions

- Get an alert by alert ID
- Get an alert by entity value
- Create an alert by entity value
- Create an alert from a transaction
- Give an alert an assessment by alert ID (check out the alert, provide a call result, and check in the alert)
- Give an alert an assessment by entity value (check out the alert, provide a call result, and check in the alert)
- Add a note to an alert by alert ID (without checking it out and with no call result added)
- Close alert by alert ID
- Close by entity value
- Close alert (by alert ID or entity value) conditionally

Analyst List Actions

- Add an entry to an analyst list by transaction
- Add a specified entry to an analyst list
- Remove an entity from an analyst list by transaction
- Remove a specified entry from an analyst list

Transaction Actions

- Mark or unmark fraudulent transactions

Unlike the IVRS interface (which requires an alert to be created before it can perform actions and is dependent on the priority of the alert within the queues and strategies), the automation interface can trigger actions using the alert ID, entity ID, or a transaction ID. This means that if certain actions need to be performed immediately (for example, send a customer notification as soon as a transaction meets the criteria of the rule), the automation interface can do so at once without having to wait for the alert to be prioritized within the queue. However, this also means that the bank’s integration layer needs to be configured to make the appropriate REST API calls.

The following table shows a list of features and how this interface is both similar to and different from the IVRS interface.

Table 1. *Feature Comparison of SAS Fraud Management Automation and IVRS Interfaces*

Feature	IVRS Interface	Automation Interface
Technology	SOAP web service calls	REST API
MQ	Not required	Not required
Integration layer	Requires the integration layer for processing data and initiating the call, or the calling system needs to be updated to send and receive SAS Fraud Management messages	Requires the integration layer for processing data and initiating the call, or the calling system needs to be updated to send and receive SAS Fraud Management messages
Speed	Slight delay in sending customer notifications due to retrieval and processing of alerts, which involves checking for new records and updates to the alert and is dependent on the alert's priority	Can send customer notifications in real time (RT) or near real time (NRT)
Alerting	Requires that an alert is created	Does not require that an alert is created; can use an alert ID, entity ID, or transaction ID to perform actions
User ID configuration	Required to perform alert actions	Required to perform alert actions
Automated manual alert creation	Incapable	Capable
Add or remove from an analyst list	Capable	Capable
Add memo to an alert using alert ID	Capable	Capable
Add memo to an alert using entity ID	Capable	Capable; there is no need to check out the alert or to add a call result
Add or remove transaction fraud markings	Capable	Capable
Close alert by alert ID	Incapable	Capable

For a full list of the actions that can be triggered through the automation interface, see the chapter "Automation Interface in *SAS Fraud Management: Message Specification*. View the Resources section of this paper to access SAS Fraud Management documentation.

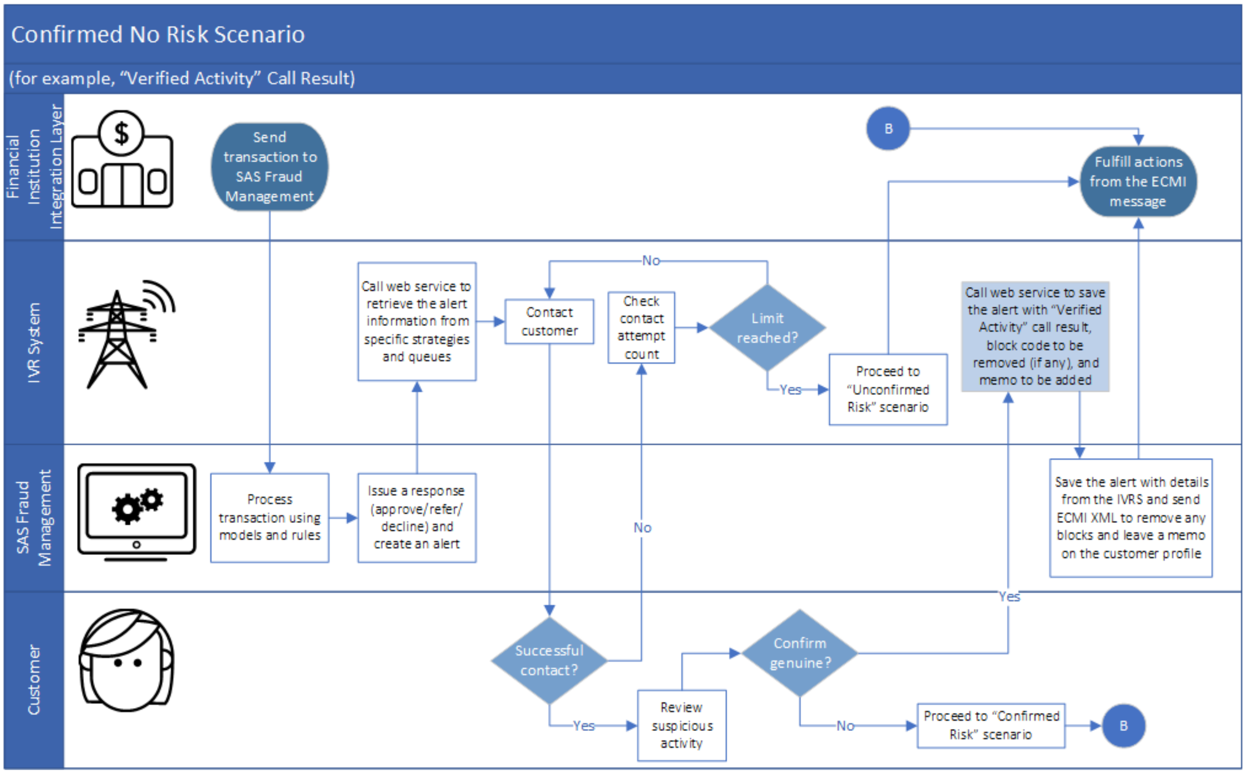
Customer Contact Process Flows via the IVRS and ECM Interfaces

The diagrams on the following pages provide examples of how the IVRS and ECMI interfaces can be leveraged to maximize the customer contact capabilities of SAS Fraud Management.

Confirmed No Risk Scenario

The following diagram shows an example of how the IVRS and ECM interfaces of SAS Fraud Management can work together in what is called a "Confirmed No Risk" scenario. In this scenario, the customer is successfully contacted by the IVRS, and confirms that the suspicious activity is genuine activity.

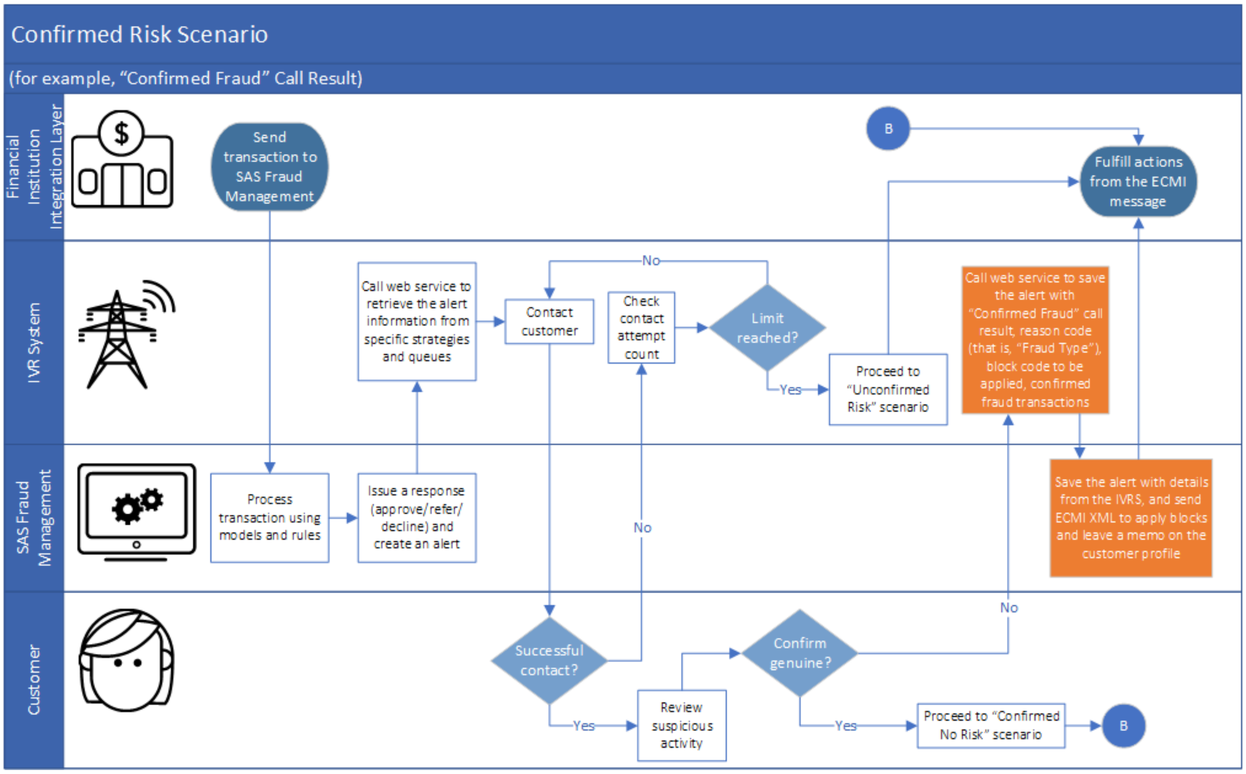
Figure 4. *Confirmed No Risk Scenario*


Confirmed No Risk Scenario
(for example, "Verified Activity" Call Result)
Financial Institution Integration Layer
IVR System
SAS Fraud Management
Customer
Send transaction to SAS Fraud Management
B
Fulfill actions from the ECMI message
Call web service to retrieve the alert information from specific strategies and queues
Contact customer
Check contact attempt count
No
Limit reached?
Yes
Proceed to "Unconfirmed Risk" scenario
Call web service to save the alert with "Verified Activity" call result, block code to be removed (if any), and memo to be added
Process transaction using models and rules
Issue a response (approve/refer/ decline) and create an alert
No
Save the alert with details from the IVRS and send ECMI XML to remove any blocks and leave a memo on the customer profile
Yes
Successful contact?
Yes
Review suspicious activity
Confirm genuine?
No
Proceed to "Confirmed Risk" scenario
B

Confirmed Risk Scenario

The following diagram shows how the IVRS and ECM interfaces of SAS Fraud Management can work together in a "Confirmed Risk" scenario. In this scenario, a customer is successfully contacted and confirms that the suspicious activity is fraudulent. The diagram is similar to the one for a "Confirmed No Risk" scenario, but the major difference lies in the processes that are highlighted in orange.

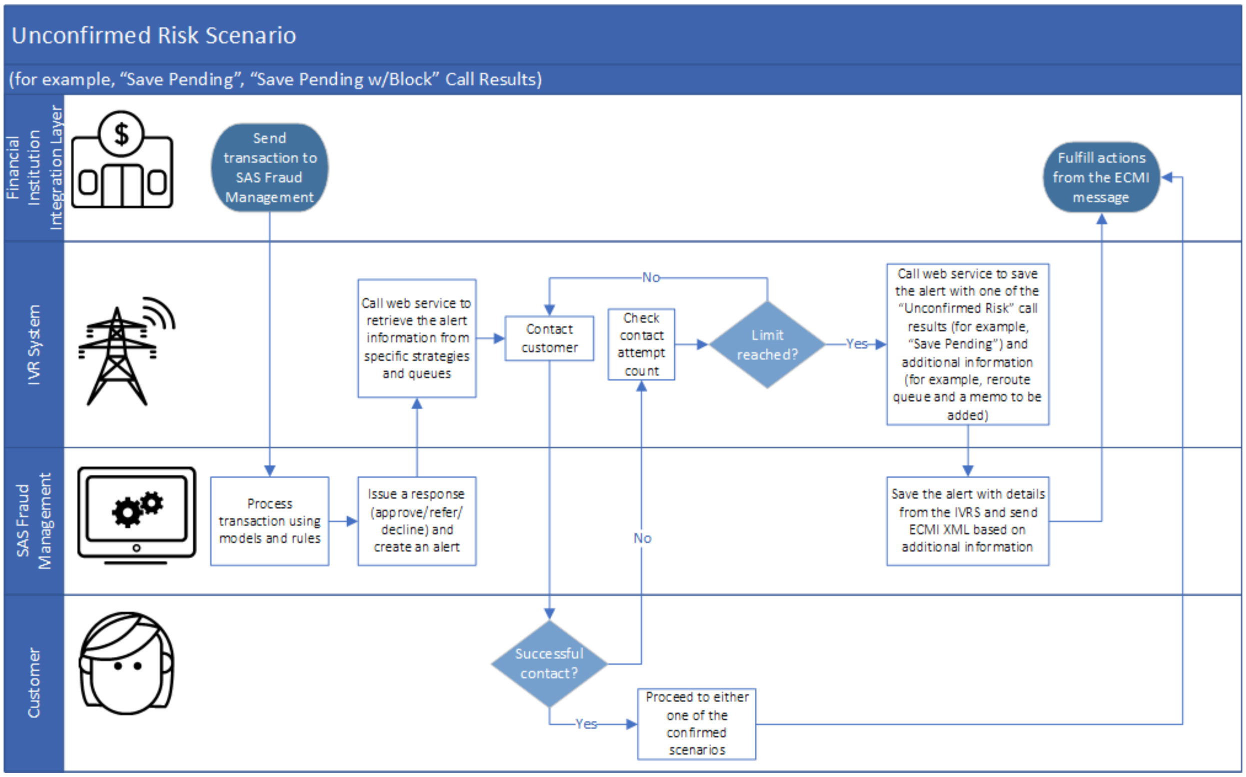
Figure 5. *Confirmed Risk Scenario*


Confirmed Risk Scenario
(for example, "Confirmed Fraud" Call Result)
Financial Institution Integration Layer
IVR System
SAS Fraud Management
Customer
$
Send transaction to SAS Fraud Management
B
Fulfill actions from the ECMI message
Call web service to retrieve the alert information from specific strategies and queues
Contact customer
Check contact attempt count
No
Limit reached?
Yes
Proceed to "Unconfirmed Risk" scenario
Call web service to save the alert with "Confirmed Fraud" call result, reason code (that is, "Fraud Type"), block code to be applied, confirmed fraud transactions
Process transaction using models and rules
Issue a response (approve/refer/decline) and create an alert
No
Save the alert with details from the IVRS, and send ECMI XML to apply blocks and leave a memo on the customer profile
No
Successful contact?
Yes
Review suspicious activity
Confirm genuine?
Yes
Proceed to "Confirmed No Risk" scenario
B

Unconfirmed Risk Scenario

However, in some cases, the IVRS is unable to contact the customer, in which case, certain actions may still need to be taken. This is what is called an "Unconfirmed Risk" scenario, and the following diagram shows how the IVRS and ECM Interfaces can still be used to handle such cases.

Figure 6. *Unconfirmed Risk Scenario*


Unconfirmed Risk Scenario
(for example, "Save Pending", "Save Pending w/Block" Call Results)
Financial Institution Integration Layer
IVR System
SAS Fraud Management
Customer
$
Send transaction to SAS Fraud Management
Process transaction using models and rules
Issue a response (approve/refer/ decline) and create an alert
Call web service to retrieve the alert information from specific strategies and queues
Contact customer
Successful contact?
No
Yes
Check contact attempt count
Limit reached?
No
Yes
Call web service to save the alert with one of the "Unconfirmed Risk" call results (for example, "Save Pending") and additional information (for example, reroute queue and a memo to be added)
Save the alert with details from the IVRS and send ECMI XML based on additional information
Fulfill actions from the ECMI message
Proceed to either one of the confirmed scenarios

Error Handling

There might be cases in which the customer's contact number might not be in the correct format that the IVRS is expecting to receive, or that the IVRS calls the web service with insufficient data to get a proper response. This is only one of the many errors that can be encountered in the process of contacting customers and servicing alerts. As a best practice, it is recommended to be prepared and have error handling processes in place.

Customer Contact Process Flows via the Automation Interface

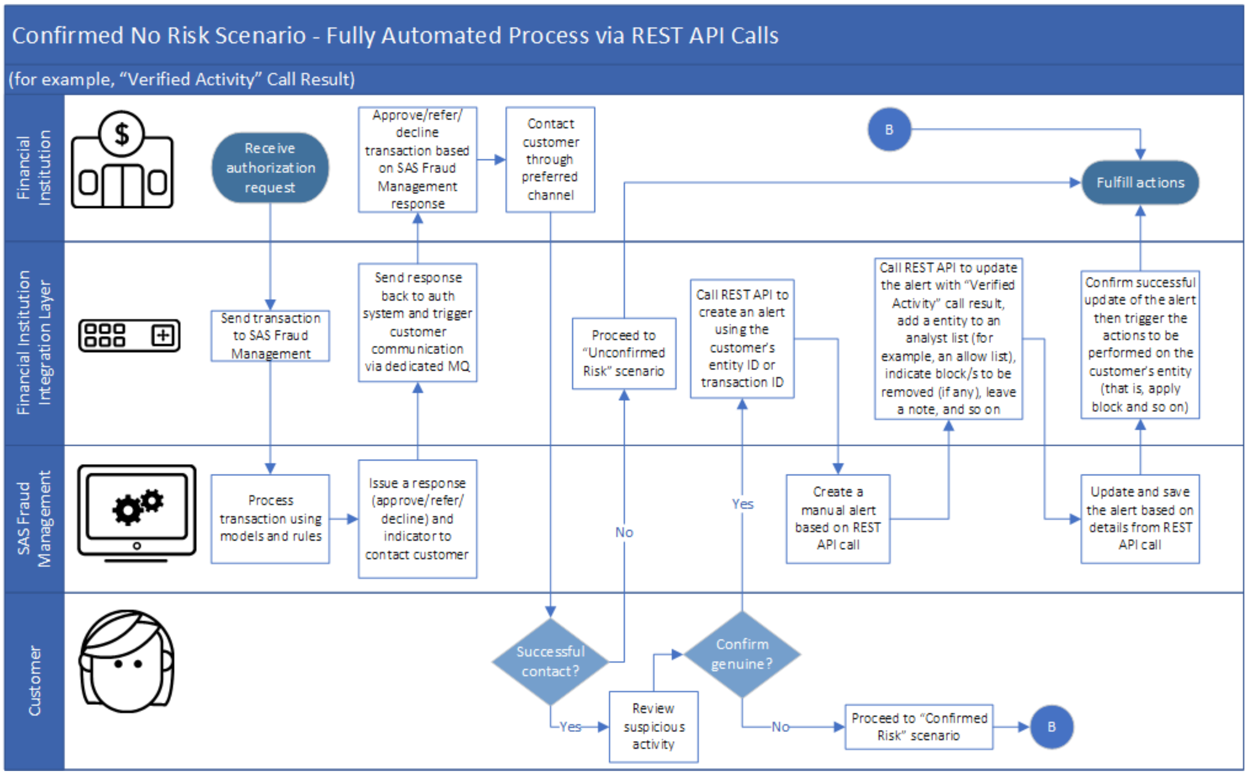
The following diagrams provide examples of how the automation interfaces can be leveraged to maximize the customer contact capabilities of SAS Fraud Management in an automated fashion.

Note: The primary difference between these process flows, and the process flows for the IVRS and ECMI interfaces is that there needs to be an integration layer to orchestrate the REST API calls.

Confirmed No Risk Scenario

The following diagram shows an example of how the SAS Fraud Management automation interface works in what is called a "Confirmed No Risk" scenario. In this scenario, the customer is successfully contacted by the IVRS, and confirms that the suspicious activity is genuine.

Figure 7. *Confirmed No Risk Scenario – Fully Automated Process via REST API Calls*

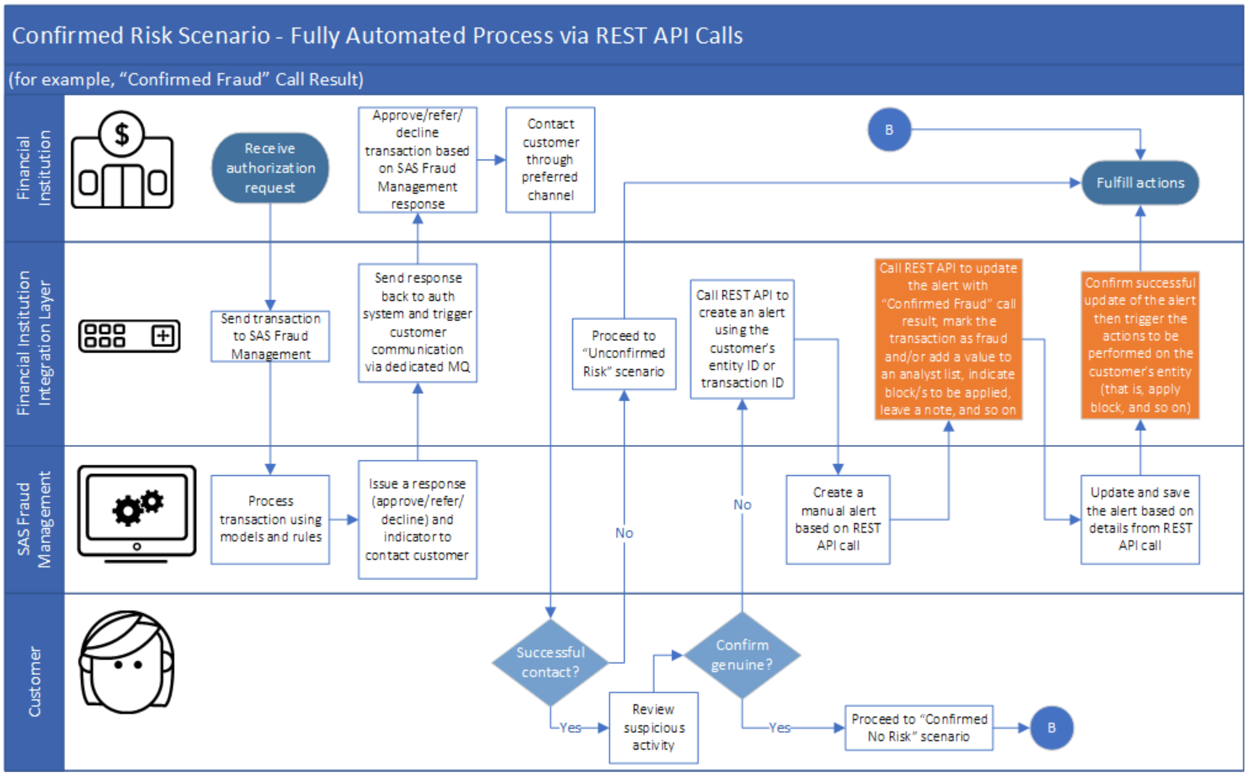


Confirmed No Risk Scenario - Fully Automated Process via REST API Calls
(for example, "Verified Activity" Call Result)
Financial Institution
Financial Institution Integration Layer
SAS Fraud Management
Customer
Receive authorization request
Approve/refer/decline transaction based on SAS Fraud Management response
Contact customer through preferred channel
B
Fulfill actions
Send transaction to SAS Fraud Management
Send response back to auth system and trigger customer communication via dedicated MQ
Proceed to "Unconfirmed Risk" scenario
Call REST API to create an alert using the customer's entity ID or transaction ID
Call REST API to update the alert with "Verified Activity" call result, add a entity to an analyst list (for example, an allow list), indicate block/s to be removed (if any), leave a note, and so on
Confirm successful update of the alert then trigger the actions to be performed on the customer's entity (that is, apply block and so on)
Process transaction using models and rules
Issue a response (approve/refer/decline) and indicator to contact customer
No
Yes
Create a manual alert based on REST API call
Update and save the alert based on details from REST API call
Successful contact?
Yes
Review suspicious activity
Confirm genuine?
No
Proceed to "Confirmed Risk" scenario
B

Confirmed Risk Scenario

The following diagram shows how the automation interface of SAS Fraud Management works in a "Confirmed Risk" scenario. In this scenario, a customer is successfully contacted and confirms that the suspicious activity is fraudulent. The diagram is similar to the one for a "Confirmed No Risk" scenario, but the major differences are highlighted in orange.

Figure 8. Confirmed Risk Scenario – Fully Automated Process via REST API Calls

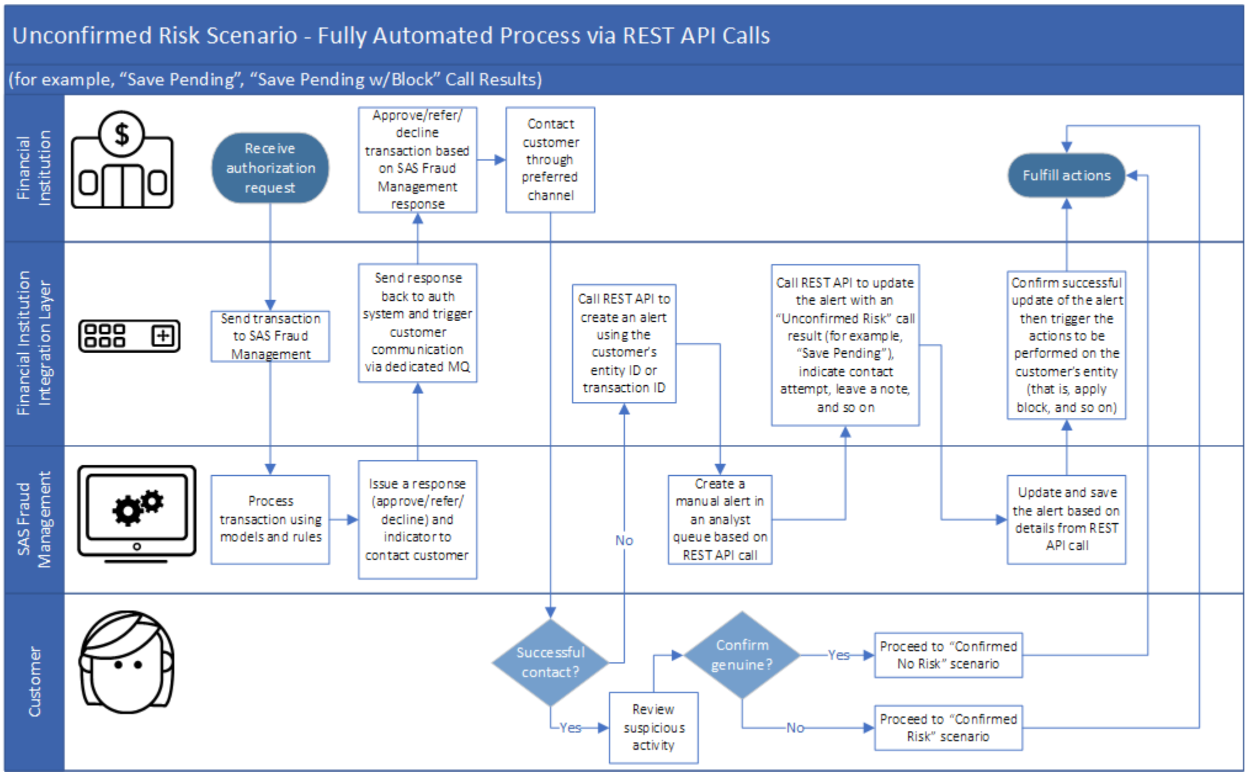


Confirmed Risk Scenario - Fully Automated Process via REST API Calls
(for example, "Confirmed Fraud" Call Result)
Financial Institution
Financial Institution Integration Layer
SAS Fraud Management
Customer
Receive authorization request
Approve/refer/ decline transaction based on SAS Fraud Management response
Contact customer through preferred channel
B
Fulfill actions
Send transaction to SAS Fraud Management
Send response back to auth system and trigger customer communication via dedicated MQ
Proceed to "Unconfirmed Risk" scenario
Call REST API to create an alert using the customer's entity ID or transaction ID
Call REST API to update the alert with "Confirmed Fraud" call result, mark the transaction as fraud and/or add a value to an analyst list, indicate block/s to be applied, leave a note, and so on
Confirm successful update of the alert then trigger the actions to be performed on the customer's entity (that is, apply block, and so on)
Process transaction using models and rules
Issue a response (approve/refer/ decline) and indicator to contact customer
No
No
Create a manual alert based on REST API call
Update and save the alert based on details from REST API call
Successful contact?
Yes
Review suspicious activity
Confirm genuine?
Yes
Proceed to "Confirmed No Risk" scenario
B

Unconfirmed Risk Scenario

In cases where the customer could not be reached in what is called an "Unconfirmed Risk" scenario, the following diagram shows how the automation interface can still be used to ensure that an alert is still attended to by a fraud analyst for assessment.

Figure 9. *Unconfirmed Risk Scenario – Fully Automated Process via REST API Calls*


Unconfirmed Risk Scenario - Fully Automated Process via REST API Calls
(for example, "Save Pending", "Save Pending w/Block" Call Results)
Financial Institution
Financial Institution Integration Layer
SAS Fraud Management
Customer
Receive authorization request
Approve/refer/decline transaction based on SAS Fraud Management response
Contact customer through preferred channel
Fulfill actions
Send transaction to SAS Fraud Management
Send response back to auth system and trigger customer communication via dedicated MQ
Call REST API to create an alert using the customer's entity ID or transaction ID
Call REST API to update the alert with an "Unconfirmed Risk" call result (for example, "Save Pending"), indicate contact attempt, leave a note, and so on
Confirm successful update of the alert then trigger the actions to be performed on the customer's entity (that is, apply block, and so on)
Process transaction using models and rules
Issue a response (approve/refer/decline) and indicator to contact customer
No
Create a manual alert in an analyst queue based on REST API call
Update and save the alert based on details from REST API call
Successful contact?
Yes
Review suspicious activity
Confirm genuine?
Yes
Proceed to "Confirmed No Risk" scenario
No
Proceed to "Confirmed Risk" scenario

References

SAS Fraud Management documentation is provided on a secure site that requires a user ID and password, which you can obtain by contacting your SAS Implementation Engineer or SAS Technical Support. In order to expedite your request, please include SAS Fraud Management in the subject field of the form.

Release Information Content Version: 1.0 October 2020.

Trademarks and Patents SAS Institute Inc. SAS Campus Drive, Cary, North Carolina 27513

To contact your local SAS office, please visit: sas.com/offices