TECHNICAL PAPER

Prescribed Environment for Payments

Last update: February 2020

Contents

Relevant Products and Releases

- *SAS® Fraud Management 6.1*

Prescribed Environment for Payments Overview

A prescribed environment is a SAS Fraud Management out-of-the-box installation. It captures industry best practices into a set of default settings and is provided as a recommendation to clients. You might use this environment as a baseline during your SAS Fraud Management implementation.

It is recommended that you review the settings associated with this document and note any changes that are required. Any changes can be made after each installation.

This document lists the business features that are provided in the payments package. The features encompass the following areas:

- Business units, groups, and teams
- Multi-organizational structure (multi-org)
- Alert types
- Strategies and queues
- Templates
- Analyst grid
- Block codes

Except for the multi-org and alert types, all the settings for these areas can be modified in the Manager's Workbench by business users (as needed) after implementation.

Changes to the multi-org and alert types need to be carefully reviewed with SAS business consultants before installation, because any changes in the future will have downstream impacts. These changes might require the assistance of SAS Technical Support. Changes to your multi-org impact user access, models, rules, and alerts. Changes to your alert types impact rule evaluation and existing alerts.

Business Units, Groups, and Teams

Business units, groups, and teams enable an organization to logically organize fraud analysts. You can change the names of business units, groups, and teams in the **Business Units** tab. Table 1 lists the default business units, groups, and teams that are provided with the prescribed environment for payments.

__Table 1.__ Business Units, Groups, and Teams

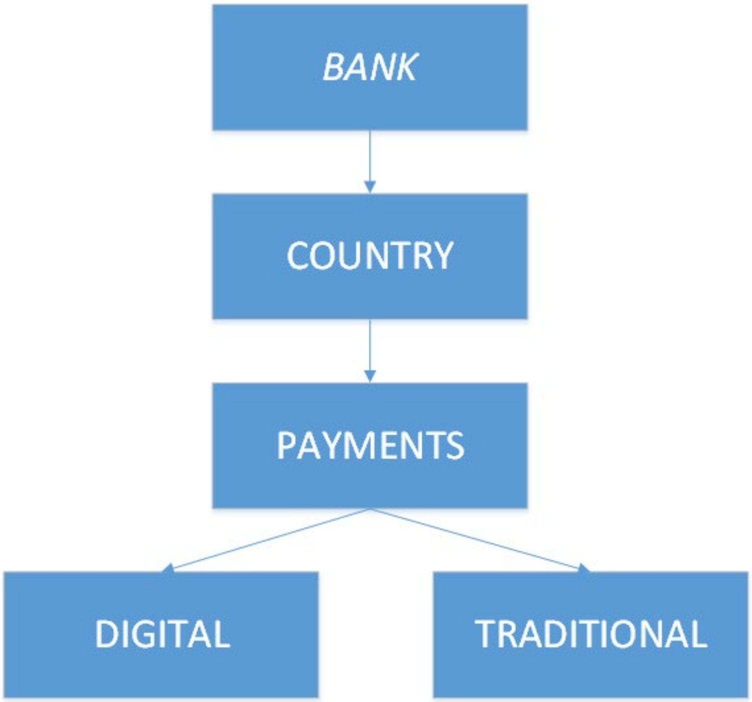
Business Units	Groups	Teams
Payments - Operations	Payment Fraud	Payment Fraud Team 1 Payment Fraud Team 2
Payment - Rule Writers	Not applicable	Not applicable

Multi-organizational Structure

Figure 1 shows the multi-org that is provided with the prescribed environment for payments.

It is recommended that you work with SAS Business Consultants if any changes to this structure need to be made before installation to ensure that this structure reflects how your business operates. Changes to your multi-org impact user access, models, rules, and alerts. A multi-org can be up to six levels deep with up to 15 child nodes on each level.

Figure 1. Levels in a Multi-organizational Structure



The Digital node would be used for any payment transactions that are performed through digital channels of the bank (for example, using the bank's online banking website, mobile phones, and so on). In the figure, the Traditional node would be used for any payment transactions that are performed through traditional banking channels (for example, branch banking or checks).

Alert Types

Table 2 shows the default alert entity structure that is provided with the prescribed environment for payments.

It is recommended that you work with SAS Business Consultants if any changes to these alert types need to be made in the future (after installation). Changes to your alert types impact rule evaluation and existing alerts.

Table 2. *Alert Types*

Usage	Level	Name	Assumed Message Layout Field
Alert working	Alert entity	PAYMENT	tpp_num
Payment linking	Parent entity	ACCOUNT	aqo_acct_num
Demographics	Contact entity	CUSTOMER	xqo_cust_num

Strategies and Queues

Strategies and queues are a way to organize and prioritize alert creation and routing. Strategies contain the queues that are populated with alerts. Strategies and queues are defined in the **Strategies** tab. Table 3 lists the default strategies and queues (and their priorities) that are provided with the prescribed environment for payments.

The priority of strategies and queues determine the following:

- Which queue an alert is created in should multiple rules fire
- The order in which queues are serviced within the Analyst Workstation. They are serviced through the following:
  - Direct servicing: Only the queue priority for the selected strategy is considered.
  - Priority servicing: The strategy and queue combination is considered.

Table 3. Strategies and Queues

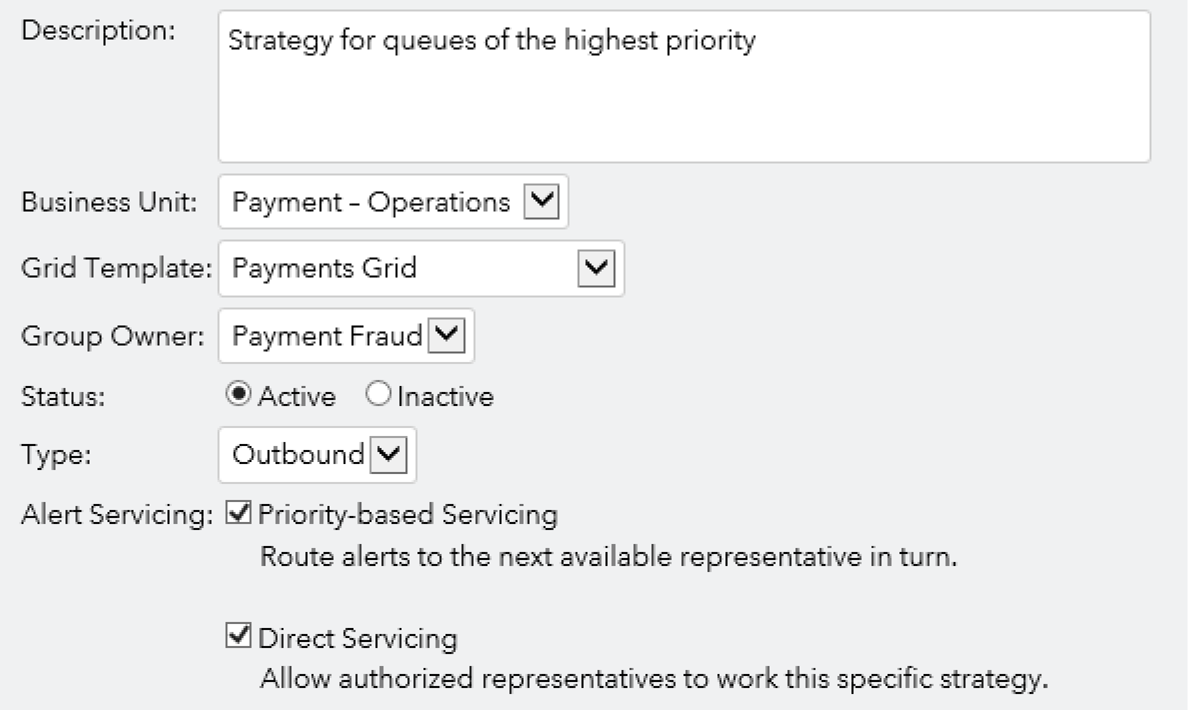
Strategy	Strategy Priority	Queue	Queue Priority
Payments - VIP	1	Payments - VIP	1
Payments - High Priority	2	Payments - Velocity Payments - High Value Payments - Phishing and Malware Payments - Account Activity/Takeover	2 3 4 5
Payments - Medium Priority	3	Payments - Log-in risk Payments - Compromised Device Payments - Hold Payments - Branch Banking	6 7 8 9
Payments - Low Priority	4	Payments - Decline	10
Payments - Manual Alerts	5	Payments - Manual Alerts	11

Note: Alerts that are created in each of the queues (except for the Payments - Manual Alerts queue) are presented to an analyst via priority servicing.

Strategy Definition: All Strategies

Figure 2 shows the default settings for all the strategies that are provided with the prescribed environment for payments.

Figure 2. Default Settings for All Strategies



Description: Strategy for queues of the highest priority

Business Unit: Payment - Operations

Grid Template: Payments Grid

Group Owner: Payment Fraud

Status: ● Active ○ Inactive

Type: Outbound

Alert Servicing: ☑ Priority-based Servicing
Route alerts to the next available representative in turn.

☑ Direct Servicing
Allow authorized representatives to work this specific strategy.

Queue Settings for Alert Creation and Routing

Table 4 shows the default queue settings for the **Alert Creation and Routing** section for all the queues that are provided with the prescribed environment for payments.

Table 4. *Default Queue Settings for Alert Creation and Routing*

	Payments - ATO	Payments - VIP	Payments - Manual Alerts	All Other Queues
Surface alerts only within the designated calling hours	✓	✓	✓	✓
Alerts in this queue are never reassigned (sticky)	✓	✓		
Allow alerts to be routed (transferred) to this queue	✓	✓		✓

	Payments - ATO	Payments - VIP	Payments - Manual Alerts	All Other Queues
Mark this queue as Inbound			✓	
Disable force checkout				

Queue Call Result Selections

Table 5 shows the call results that have been defined for all the queues that are provided with the prescribed environment for payments.

Table 5. *Call Results for All Queues*

Call Result Type	Call Result	Payments - Manual Alerts	All other Queues
UNCONFIRMED RISK	SKIP		
	RESCHEDULE		✓
	SAVE PENDING		✓
	SAVE PENDING WITH BLOCK		✓
	REROUTE	✓	✓
	ASSUMED GENUINE		✓
	ASSUMED FRAUD		✓
CONFIRMED NO RISK	VERIFIED ACTIVITY	✓	✓

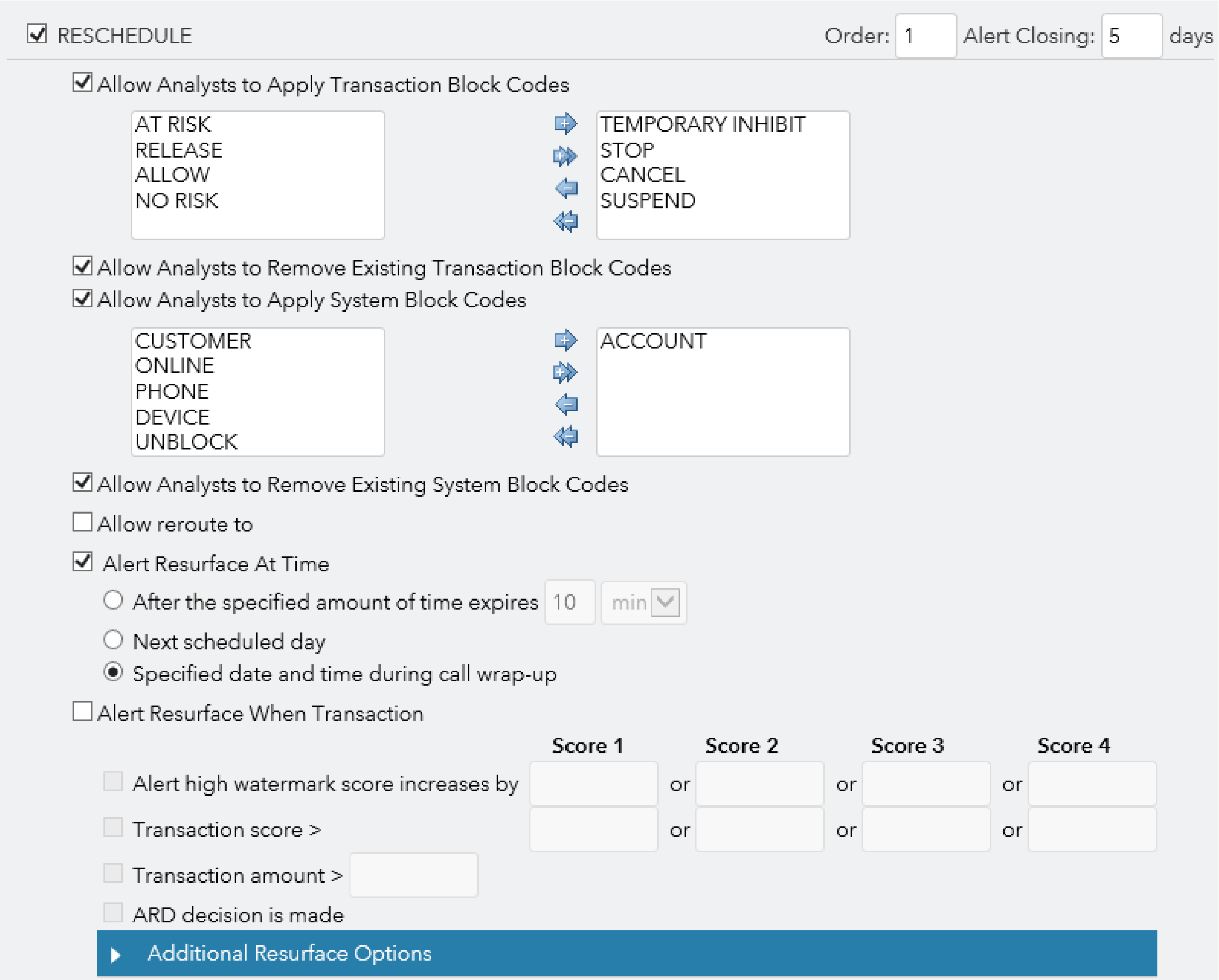
Call Result Type	Call Result	Payments - Manual Alerts	All other Queues
CONFIRMED RISK	CONFIRMED FRAUD	✓	✓

Call Queue Result Settings

RESCHEDULE

Fraud analysts will use Figure 3, the RESCHEDULE call result, when they want to set a specific date and time at which an alert should resurface. Fraud analysts also have the option to add transaction block codes and system block codes in case they determine that the suspicious activity in the alert has a high risk of fraud.

Figure 3. RESCHEDULE Call Result



☑ RESCHEDULE — Order: 1 Alert Closing: 5 days

☑ Allow Analysts to Apply Transaction Block Codes

AT RISK RELEASE ALLOW NO RISK	TEMPORARY INHIBIT STOP CANCEL SUSPEND

☑ Allow Analysts to Remove Existing Transaction Block Codes

☑ Allow Analysts to Apply System Block Codes

CUSTOMER ONLINE PHONE DEVICE UNBLOCK	ACCOUNT

☑ Allow Analysts to Remove Existing System Block Codes

□ Allow reroute to

☑ Alert Resurface At Time

- ○ After the specified amount of time expires 10 min
- ○ Next scheduled day
- ● Specified date and time during call wrap-up

□ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
□ Alert high watermark score increases by		or		or		or	
□ Transaction score >		or		or		or	

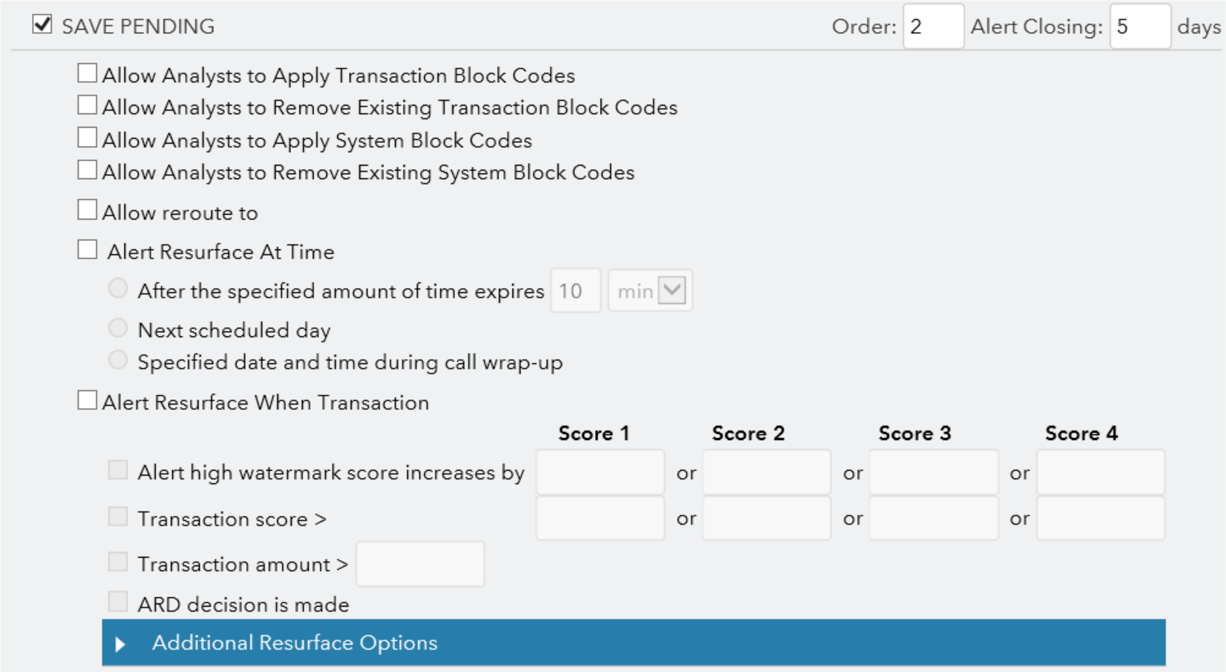
□ Transaction amount >

□ ARD decision is made

SAVE PENDING

Fraud analysts will use Figure 4, the SAVE PENDING call result, when they do not have enough information to determine the riskiness or the legitimacy of the activity and would not apply or remove a block on the transaction or account.

Figure 4. SAVE PENDING Call Result with Insufficient Information



☑ SAVE PENDING — Order: 2 — Alert Closing: 5 days

□ Allow Analysts to Apply Transaction Block Codes
□ Allow Analysts to Remove Existing Transaction Block Codes
□ Allow Analysts to Apply System Block Codes
□ Allow Analysts to Remove Existing System Block Codes
□ Allow reroute to
□ Alert Resurface At Time
○ After the specified amount of time expires 10 min
○ Next scheduled day
○ Specified date and time during call wrap-up
□ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
□ Alert high watermark score increases by		or		or		or	
□ Transaction score >		or		or		or	

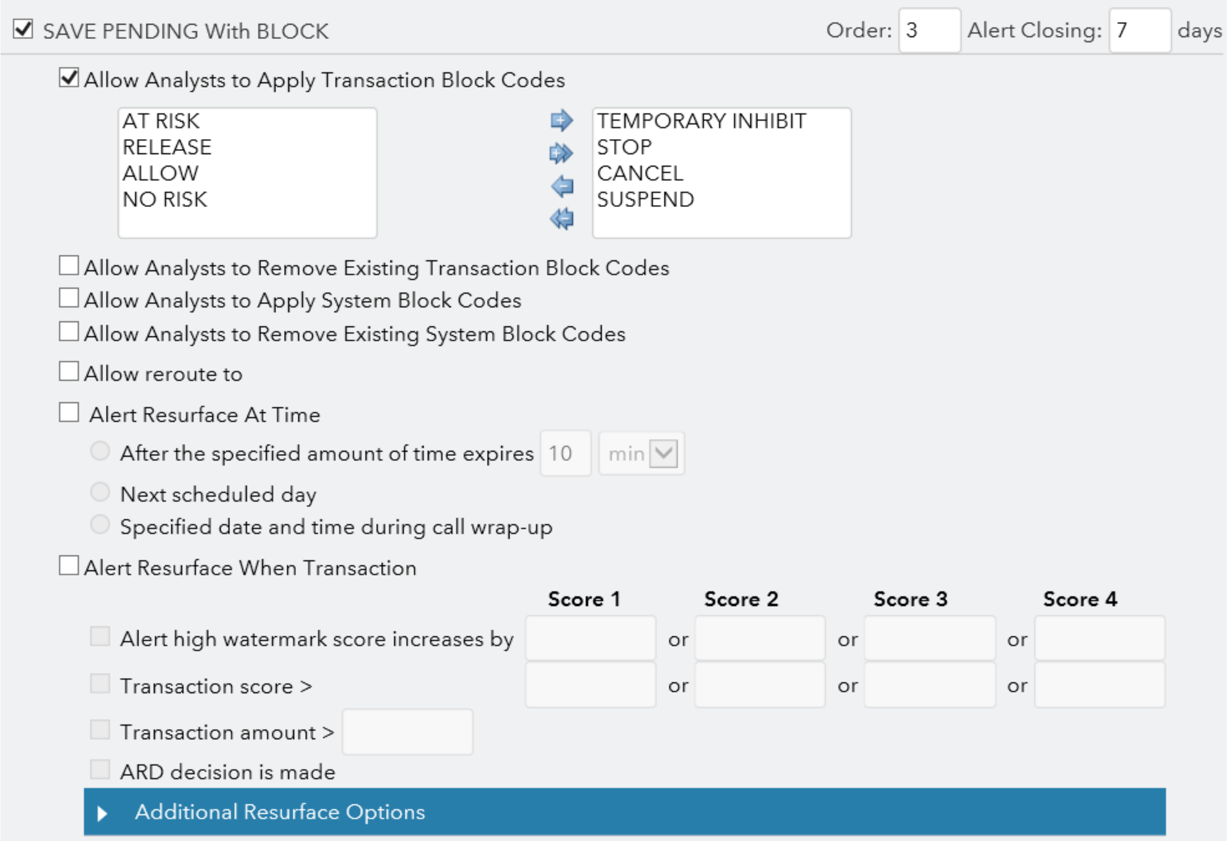
□ Transaction amount >
□ ARD decision is made

▸ Additional Resurface Options

SAVE PENDING with BLOCK

Fraud analysts will use Figure 5, the SAVE PENDING with BLOCK call result, when they have reasonable doubt to block the suspicious activity, but do not have enough information to assume that it is fraud.

Figure 5. SAVE PENDING with BLOCK Call Result



☑ SAVE PENDING With BLOCK — Order: 3 — Alert Closing: 7 days

☑ Allow Analysts to Apply Transaction Block Codes

AT RISK RELEASE ALLOW NO RISK	TEMPORARY INHIBIT STOP CANCEL SUSPEND

☐ Allow Analysts to Remove Existing Transaction Block Codes

☐ Allow Analysts to Apply System Block Codes

☐ Allow Analysts to Remove Existing System Block Codes

☐ Allow reroute to

☐ Alert Resurface At Time

- ○ After the specified amount of time expires 10 min
- ○ Next scheduled day
- ○ Specified date and time during call wrap-up

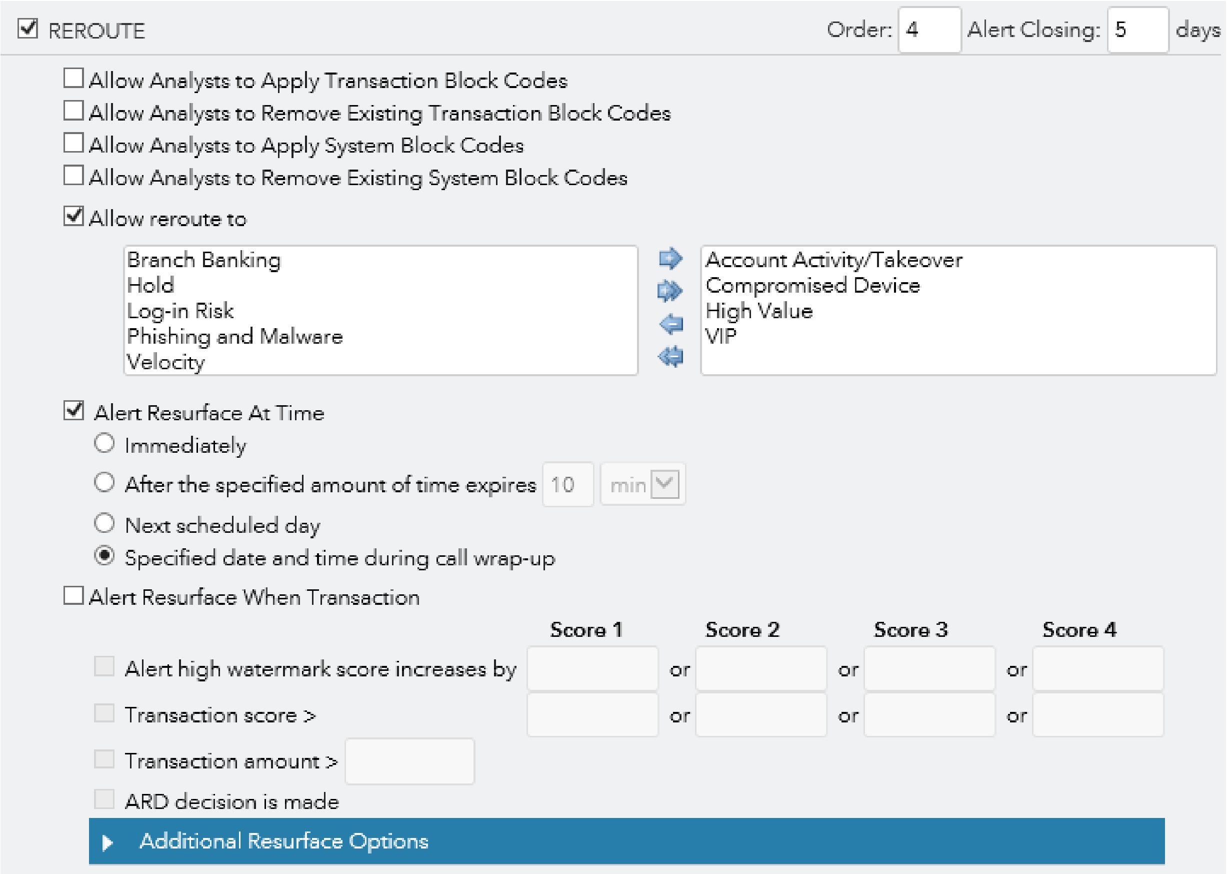
☐ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
☐ Alert high watermark score increases by		or		or		or	
☐ Transaction score >		or		or		or	
☐ Transaction amount >							
☐ ARD decision is made							

REROUTE

Fraud analysts will use Figure 6, the REROUTE call result, when they determine that the alert should be routed to a different queue, which requires special handling (for example, a VIP client or high risk of identity theft fraud). No other action is allowed on the alert.

Figure 6. REROUTE Call Result



☑ REROUTE — Order: 4 — Alert Closing: 5 days

□ Allow Analysts to Apply Transaction Block Codes
□ Allow Analysts to Remove Existing Transaction Block Codes
□ Allow Analysts to Apply System Block Codes
□ Allow Analysts to Remove Existing System Block Codes

☑ Allow reroute to

Branch Banking Hold Log-in Risk Phishing and Malware Velocity	Account Activity/Takeover Compromised Device High Value VIP

☑ Alert Resurface At Time
○ Immediately
○ After the specified amount of time expires 10 min
○ Next scheduled day
● Specified date and time during call wrap-up

□ Alert Resurface When Transaction

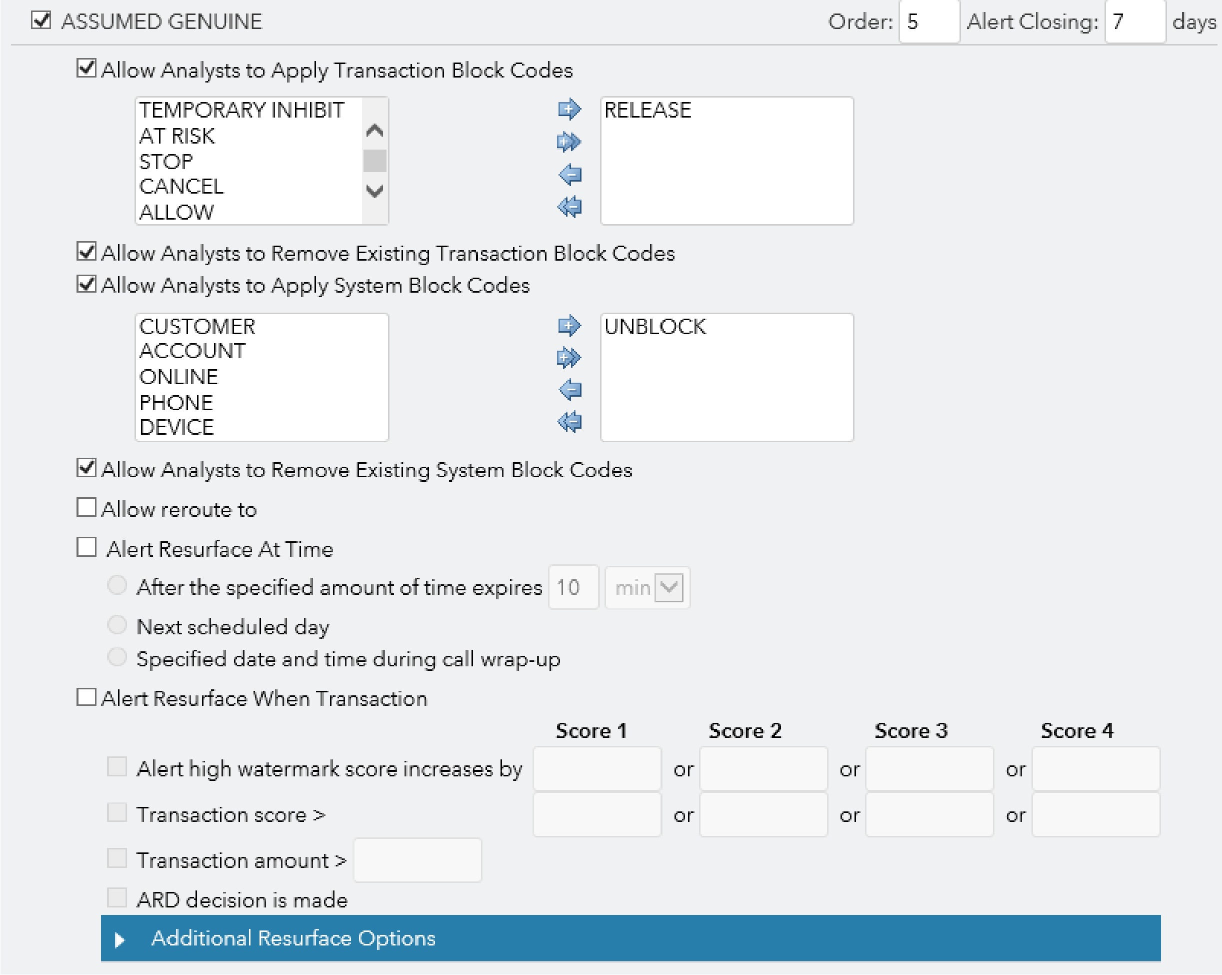
	Score 1		Score 2		Score 3		Score 4
□ Alert high watermark score increases by		or		or		or	
□ Transaction score >		or		or		or	
□ Transaction amount >							
□ ARD decision is made							

▶ Additional Resurface Options

ASSUMED GENUINE

Fraud analysts will use the Figure 7, ASSUMED GENUINE call result, when they have sufficient information to assume the legitimacy of the activity in the alert but have not yet confirmed this with the customer.

Figure 7. ASSUME GENUINE Call Result



☑ ASSUMED GENUINE Order: 5 Alert Closing: 7 days

☑ Allow Analysts to Apply Transaction Block Codes

TEMPORARY INHIBIT AT RISK STOP CANCEL ALLOW	RELEASE

☑ Allow Analysts to Remove Existing Transaction Block Codes

☑ Allow Analysts to Apply System Block Codes

CUSTOMER ACCOUNT ONLINE PHONE DEVICE	UNBLOCK

☑ Allow Analysts to Remove Existing System Block Codes

☐ Allow reroute to

☐ Alert Resurface At Time

○ After the specified amount of time expires 10 min

○ Next scheduled day

○ Specified date and time during call wrap-up

☐ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
☐ Alert high watermark score increases by		or		or		or	
☐ Transaction score >		or		or		or	

☐ Transaction amount >

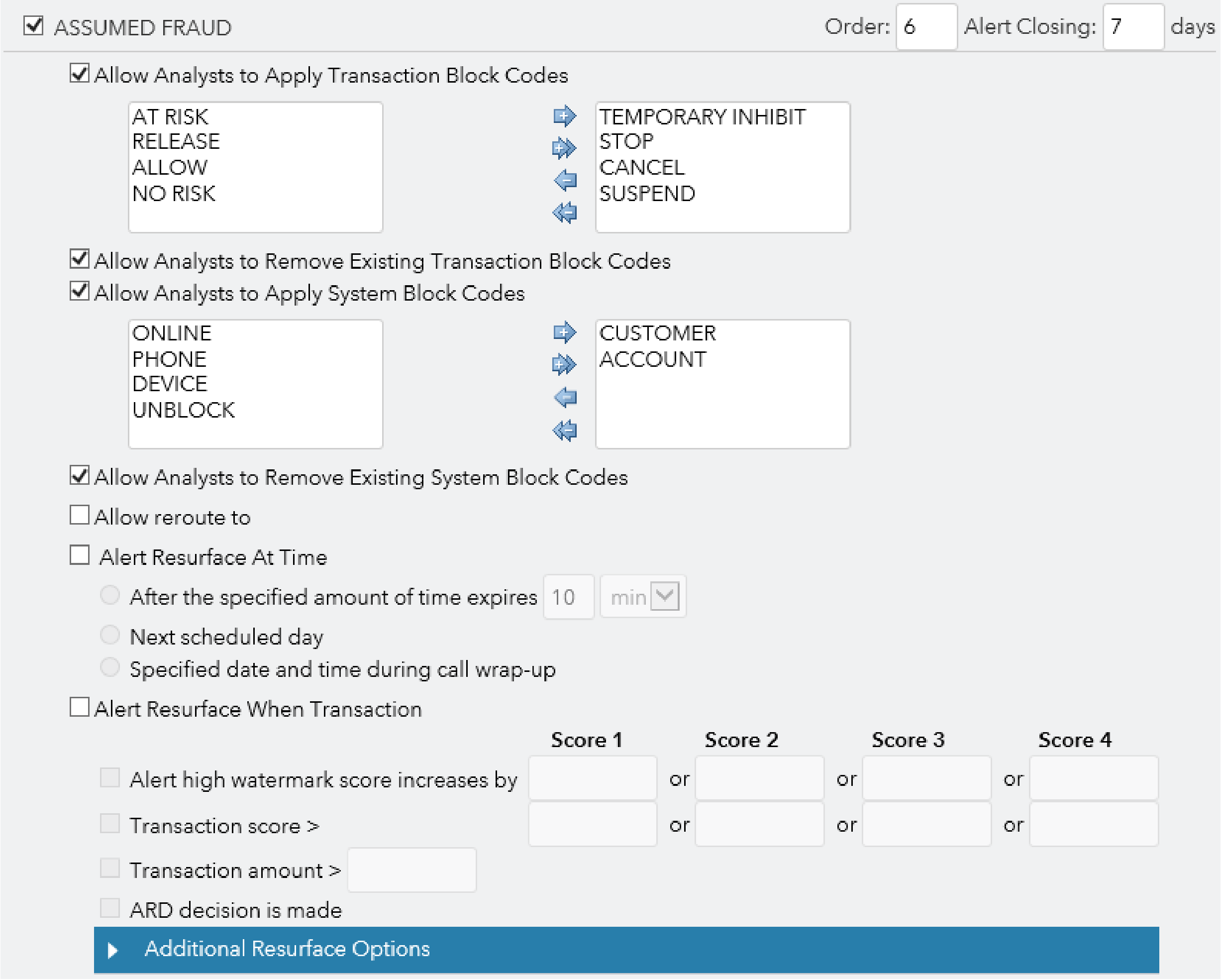
☐ ARD decision is made

▸ Additional Resurface Options

ASSUMED FRAUD

Fraud analysts will use Figure 8, the ASSUMED FRAUD call result, when they have sufficient information to assume that the suspicious activity in the alert is fraudulent but have not yet confirmed this with the customer.

Figure 8. ASSUMED FRAUD Call Result



☑ ASSUMED FRAUD   Order: 6   Alert Closing: 7 days

☑ Allow Analysts to Apply Transaction Block Codes

AT RISK
RELEASE
ALLOW
NO RISK

TEMPORARY INHIBIT
STOP
CANCEL
SUSPEND

☑ Allow Analysts to Remove Existing Transaction Block Codes

☑ Allow Analysts to Apply System Block Codes

ONLINE
PHONE
DEVICE
UNBLOCK

CUSTOMER
ACCOUNT

☑ Allow Analysts to Remove Existing System Block Codes

☐ Allow reroute to

☐ Alert Resurface At Time

○ After the specified amount of time expires 10 min

○ Next scheduled day

○ Specified date and time during call wrap-up

☐ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
☐ Alert high watermark score increases by		or		or		or	
☐ Transaction score >		or		or		or	

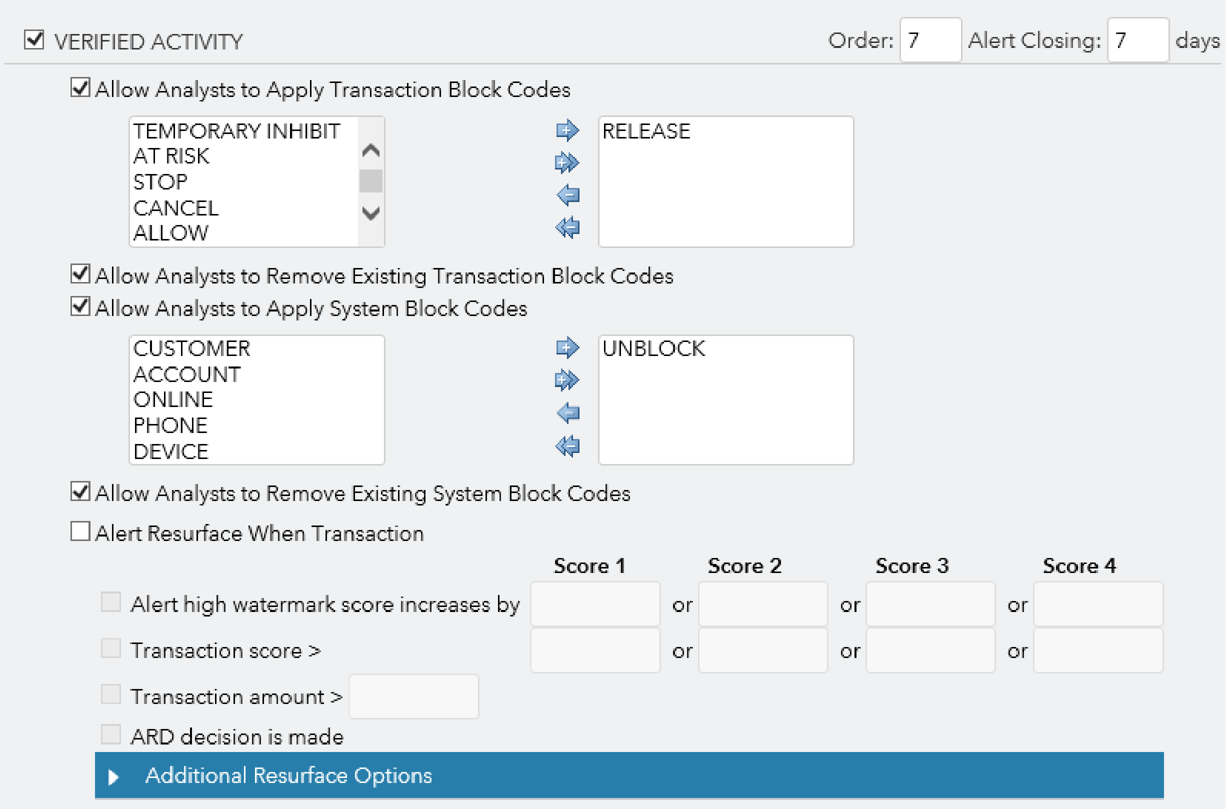
☐ Transaction amount >

☐ ARD decision is made

VERIFIED ACTIVITY

Fraud analysts will use Figure 9, the VERIFIED ACTIVITY call result, only when they have confirmed the legitimacy of the activity with the customer.

Figure 9. VERIFIED ACTIVITY Call Result



☑ VERIFIED ACTIVITY Order: 7 Alert Closing: 7 days

☑ Allow Analysts to Apply Transaction Block Codes

TEMPORARY INHIBIT
AT RISK
STOP
CANCEL
ALLOW

RELEASE

☑ Allow Analysts to Remove Existing Transaction Block Codes

☑ Allow Analysts to Apply System Block Codes

CUSTOMER
ACCOUNT
ONLINE
PHONE
DEVICE

UNBLOCK

☑ Allow Analysts to Remove Existing System Block Codes

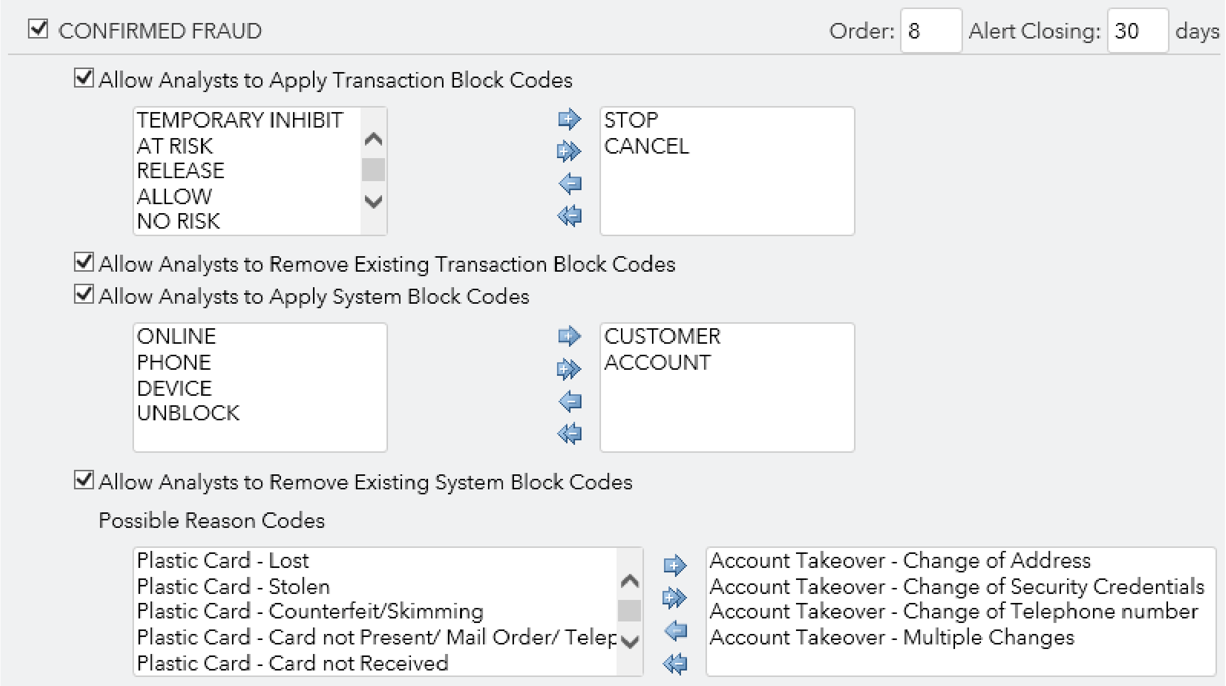
□ Alert Resurface When Transaction

	Score 1		Score 2		Score 3		Score 4
□ Alert high watermark score increases by		or		or		or	
□ Transaction score >		or		or		or	
□ Transaction amount >							
□ ARD decision is made							

CONFIRMED FRAUD

Fraud analysts will use Figure 10, the CONFIRMED FRAUD call result, only when they have confirmed with the customer that the suspicious activity in the alert was unauthorized (that is, fraudulent). Possible fraud types include (depending on the fraud type to be addressed by the strategy) non-card fraud type, all available check, payment, account takeover, scam, phishing, and so on.

Figure 10. CONFIRMED FRAUD Call Result



☑ CONFIRMED FRAUD   Order: 8   Alert Closing: 30 days

☑ Allow Analysts to Apply Transaction Block Codes

TEMPORARY INHIBIT AT RISK RELEASE ALLOW NO RISK	STOP CANCEL

☑ Allow Analysts to Remove Existing Transaction Block Codes

☑ Allow Analysts to Apply System Block Codes

ONLINE PHONE DEVICE UNBLOCK	CUSTOMER ACCOUNT

☑ Allow Analysts to Remove Existing System Block Codes

Possible Reason Codes

Plastic Card - Lost Plastic Card - Stolen Plastic Card - Counterfeit/Skimming Plastic Card - Card not Present/ Mail Order/ Telep Plastic Card - Card not Received	Account Takeover - Change of Address Account Takeover - Change of Security Credentials Account Takeover - Change of Telephone number Account Takeover - Multiple Changes

Block Codes

Table 6 lists the default block codes (and their associated block types and block labels) that are defined and assigned in the prescribed environment for payments. Block codes are defined in the **Tables** tab.

The transaction block codes are intended to block a specific type of transaction. System block codes are intended to block an entity’s transaction. However, you can determine how each block code will be used. It is recommended that these block codes remain consistent with the block codes that are used in your internal systems.

Note: Your internal systems must be configured to accept these block codes.

Table 6. *Default Block Codes That Are Assigned*

Block Code	Block Type	Block Label	Block Owner
TMPINH	Transaction	TEMPORARY INHIBIT	FA
RELEASE	Transaction	RELEASE	FA
STP	Transaction	STOP	FA
CNCL	Transaction	CANCEL	FA
SUSPND	Transaction	SUSPEND	FA
CSTBLK	System	CUSTOMER	FA
ACCBLK	System	ACCOUNT	FA
ONLBLK	System	ONLINE	FA
PHNBLK	System	PHONE	FA
DVCBLK	System	DEVICE	FA
UNBLK	System	UNBLOCK	FA

Templates

In the **Templates** tab, you can define or modify memos and call scripts, and you can associate email, letter, and SMS text message templates with a business unit.

Memos

Table 7 lists the memos that are provided with the prescribed environment for payments.

Table 7. *Predefined Memo Assignment*

Memo Name	Text
Payments - Fraudulent Activity	Customer confirmed that activity from {date} was unrecognized. Temporary block applied. Customer passed to specialist team.
Payments - Genuine Activity	Customer confirms that the activity on {date} is genuine. No further action.
Payments - Unconfirmed activity - block applied	Customer could not be contacted. Messages left on cellular, home, and work voicemails to initiate a response. Upon contact please confirm transactions from {date}. {XX} Block applied.
Payments - Unconfirmed activity - no block applied	Customer could not be contacted. Messages left on cellular, home, and work voicemails to initiate a response. Upon contact please confirm transactions from {date}.

Call Scripts

Table 8 lists the call scripts that are provided with the prescribed environment for payments.

Table 8. *Call Scripts with Predefined Memo Assignment*

Call Script Name	Text
Payments - Fraud Alert	Good morning/afternoon/evening & contact_fullName. I am calling you today from {BANK}. Our fraud detection system has highlighted potentially risky behavior following recent activity seen through the {BANK} banking system. I would like to confirm some recent activity with you.

Call Script Name	Text
Payments - Leave Voicemail	Hello, this is a message for &contact full Name from {BANK}. Please can you contact us regarding & demographic_accountType at your earliest convenience. Thank you.

Analyst Grid Templates

The analyst grid on the Alert page shows a list of a customer’s most recent transactions. Analyst transaction grids are defined in the **Preferences** tab. For more information about Analyst Grids, see *SAS Fraud Management: Manager’s Workbench User’s Guide*.

The following lists the accounts (of the customer) that are covered in the default Payments Grid:

- Checking/Savings Account
- Credit Card Account

The following lists the activities on the accounts (mentioned above) that are covered in the default Payments Grid:

- Bill Payment/Fund Transfer to Third Party or Self-Account
- Bill Payment/Fund Transfer Scheduling and Cancellation
- Check Payment
- Non-monetary

Table 9 lists the fields that appear on the analyst transaction grid for Checking/Savings Account Bill Payment/Fund Transfer to Third Party or Self-Account (CheckSavAcct > BillPay).

Table 9. *Checking/Savings Account Bill Payment/Fund Transfer to Third Party or Self-Account*

Column Name	Column Description
rqo_tran_date_alt	Date of the transaction for display. This value is client driven.
rqo_tran_time_alt	hhmmssth - Time of the transaction for display. This value is client driven.

Column Name	Column Description
rrr_action_code	n - Final A-R-D decision including SAS OnDemand Scoring Engine and external decision factors. These values are in order of restrictiveness: 0: Unknown or not applicable. 1: Approved. 2: Verification. 3: Referral. 4: Decline. 5: Pickup. 6: Ignore.
last_rule_fired	The last rule that fired on the transaction.
all_rules_fired	All rules that fired on the transaction.
aqo_acct_num	Account number of the primary interest (for example, the transacting account for payment card transactions).
hbp_type	Processing type. Convention: B: Batch. R: Real time.

Column Name	Column Description
hbp_application	Processing application. Convention: A: ATM Banking (Details unknown, insufficient information to populate channel and authentication components, as in the case of many ATM deposits or payments made at ATMs). C: Mail or correspondence (Details unknown, insufficient information to populate channel and authentication components). E: EFT processing. H: Branch banking (Details unknown, insufficient information to populate channel and authentication components). M: Maintenance. O: Online banking (Details unknown, insufficient information to populate channel and authentication components). P: Phone banking (Details unknown, insufficient information to populate channel and authentication components). Q: Check clearing. R: Other banking (Details unknown, insufficient information to populate channel and authentication components). U: Unknown.
hbp_date	Date of processing.
tbt_tran_type	Transaction type. Convention: B: Bill payment. T: Fund transfer. K: Bulk fund transfer. W: Wire transfer. P: Peer-to-peer payment.

Column Name	Column Description
tbt_ref_num	Unique ID of the transaction.
tbt_tran_status	Transaction status. Convention: A: Approved or successful. B: Canceled by the bank. C: Canceled by the customer. D: Declined or unsuccessful. P: Pending. R: Reversal.
tbt_revision_code	Revision code. Convention: C: Changed. D: Deleted. O: Original.
tbt_billing_amt	Transaction amount in billing currency (aqo_billing_curr_code) and in scientific notation. This value should always be a positive number.
tbt_tran_amt	Transaction amount in transaction currency and in scientific notation. This value should always be a positive number
tbt_tran_curr_code	Three-digit numeric ISO code of transaction currency. (Do not truncate leading zeros.)
tbt_direct_debt_ind	Direct debit indicator. Valid values are Y and N.
tbt_self_acct_ind	Transfer to self-account indicator. Valid values are Y and N.

Column Name	Column Description
tbt_bill_cat	Bill category for bill payment. Convention: CA: Credit card account payment. ED: Education. ML: Mortgage or loan payment. IS: Insurance. OT: Other. (not classified). SU: Subscription. SV: Services. TE: Telecommunication. UT: Utilities. Blank: Not applicable.
tbt_billing_ref_num	Billing reference number (for example, payer account number, subscription ID, and so on).
tpp_payee_payer_ind	Payee or payer indicator. Convention: D: Designated payee. E: Payee. N: Non-designated payee. R: Payer.
tpp_entity_type	Type of entity. Convention: A: Third-party name and address only. C: Self-cell or mobile phone. D: Third-party cell or mobile phone. E: Email. M: Merchant. N: Social network ID. P: Package accounts. S: Self-bank account. T: Third-party bank account.
tpp_name	Payee or payer’s name.

Column Name	Column Description
tpp_acct_num	Account number.
tpp_bank_cntry_code	Account bank country.
tpp_bank_num	Account bank number.
tpp_bank_name	Account bank name.
hob_ip_address	IP address.
hob_ip_address_v6	IP address v6.
hob_ip_cntry_code	Three-digit ISO country code representing the location of the IP address.
hob_device	Online banking device type. Convention: A: Mobile phone app. C: Computer. M: Mobile phone browser.
hqo_ob_userid	Online or internet banking user ID.
hdf_dev_fp_val	Device fingerprint hash string.

Table 10 lists the fields that appear on the analyst transaction grid for Checking/Savings Account Bill Payment/Fund Transfer Scheduling and Cancellation (CheckSavAcct > BillPaySched).

Table 10. *Checking/Savings Account Bill Payment/Fund Transfer Scheduling and Cancellation*

Column Name	Column Description
rqo_tran_date_alt	Date of the transaction for display. This value is client driven.
rqo_tran_time_alt	hhmmssth - Time of the transaction for display. This value is client driven.
rrr_action_code	n - Final A-R-D decision including SAS OnDemand Scoring Engine and external decision factors. These values are in order of restrictiveness: 0: Unknown or not applicable. 1: Approved. 2: Verification. 3: Referral. 4: Decline. 5: Pickup. 6: Ignore.
last_rule_fired	The last rule that fired on the transaction.
all_rules_fired	All rules that fired on the transaction.
aqo_acct_num	Account number of the primary interest (for example, the transacting account for payment card transactions).
tsh_ref_num	Transaction reference number.

Column Name	Column Description
tsh_tran_status	Scheduling status. Convention: A: Approved or successful. B: Canceled by the bank or a reversal. C: Canceled by the customer. D: Declined or unsuccessful. P: Pending.
tsh_revision_code	Revision code. Convention: C: Changed. D: Deleted. O: Original.
tsh_amount_type	Type of transaction amount. Convention: F: Fixed amount. M: Minimum due. P: Paid In full.
tsh_billing_amt	Transaction amount in billing currency and in scientific notation. This should always be a positive number.
tsh_client_amt	Transaction amount in client amount in scientific notation. This should always be a positive number.
tsh_client_curr_code	Three-digit numeric ISO currency code. (Do not truncate leading zeros.)
tsh_sch_start_date	Scheduled payment start date.
tsh_sch_end_date	Scheduled payment end date.

Column Name	Column Description
tsh_recurr_freq	Recurring frequency. Convention: 1: Once. A: Annually. D: Daily. M: Monthly. N: Month-end. Q: Quarterly. S: Semi-annually. W: Weekly.
tsh_self_acct_ind	Transfer between self-account indicator. Valid values are Y and N.
tsh_bill_cat	Bill category for bill payment. Convention: CA: Credit card account payment. ED: Education. ML: Mortgage or loan payment. IS: Insurance. OT: Other. (not classified). SU: Subscription. SV: Services. TE: Telecommunication. UT: Utilities. Blank: Not applicable.
tsh_billing_ref_num	Billing reference number (for example, payer account number, subscription ID, and so on).
tpp_payee_payer_ind	Payee or payer indicator. Convention: D: Designated payee. E: Payee. N: Non-designated payee. R: Payer.

Column Name	Column Description
tpp_entity_type	Type of entity. Convention: A: Third-party name and address only. C: Self-cell or mobile phone. D: Third-party cell or mobile phone. E: Email. M: Merchant. N: Social network ID. P: Package accounts. S: Self-bank account. T: Third-party bank account.
tpp_name	Payee or payer's name.
tpp_acct_num	Account number.
tpp_bank_cntry_code	Account bank country.
tpp_bank_num	Account bank number.
tpp_bank_name	Account bank name.
hob_ip_address	IP address.
hob_ip_address_v6	IP address v6.
hob_ip_cntry_code	Three-digit ISO country code representing the location of the IP address.

Column Name	Column Description
hob_device	Online banking device type. Convention: A: Mobile phone app. C: Computer. M: Mobile phone browser.
hdf_dev_fp_val	Device fingerprint hash string.

Table 11 lists the fields that appear on the analyst transaction grid for Checking/Savings Account (CheckSavAcct > CheckPay).

Table 11. *Checking/Savings Account*

Column Name	Column Description
rqo_tran_date_alt	Date of the transaction for display. This value is client driven.
rqo_tran_time_alt	hhmmssth - Time of the transaction for display. This value is client driven.
rrr_action_code	n - Final A-R-D decision including SAS OnDemand Scoring Engine and external decision factors. These values are in order of restrictiveness: 0: Unknown or not applicable. 1: Approved. 2: Verification. 3: Referral. 4: Decline. 5: Pickup. 6: Ignore.
last_rule_fired	The last rule that fired on the transaction.

Column Name	Column Description
all_rules_fired	All rules that fired on the transaction.
aqo_acct_num	Account number of the primary interest (for example, the transacting account for payment card transactions).
hbp_type	Processing type. Convention: B: Batch. R: Real time.
hbp_application	Processing application. Convention: A: ATM Banking (Details unknown, insufficient information to populate channel and authentication components, as in the case of many ATM deposits or payments made at ATMs). C: Mail or correspondence (Details unknown, insufficient information to populate channel and authentication components). E: EFT processing. H: Branch banking (Details unknown, insufficient information to populate channel and authentication components). M: Maintenance. O: Online banking (Details unknown, insufficient information to populate channel and authentication components). P: Phone banking (Details unknown, insufficient information to populate channel and authentication components). Q: Check clearing. R: Other banking (Details unknown, insufficient information to populate channel and authentication components). U: Unknown.

Column Name	Column Description
hbp_date	Date of processing.
tck_tran_status	Check transaction status. Convention: R: Rejected. N: Normal.
tck_status_reason	Client-defined status reason.
tck_ref_num	Transaction reference number.
tck_billing_amt	Transaction amount in billing currency and in scientific notation. This value should always be a positive number.
tck_client_amt	Transaction amount in client amount in scientific notation. This value should always be a positive number
tck_client_curr_code	Three-digit numeric ISO currency code. (Do not truncate leading zeros.)
tpp_payee_payer_ind	Payee or payer indicator. Convention: D: Designated payee. E: Payee. N: Non-designated payee. R: Payer.

Column Name	Column Description
tpp_entity_type	Type of entity. Convention: A: Third-party name and address only. C: Self-cell or mobile phone. D: Third-party cell or mobile phone. E: Email. M: Merchant. N: Social network ID. P: Package accounts. S: Self-bank account. T: Third-party bank account.
tpp_name	Payee or payer's name.
tpp_acct_num	Account number.
tpp_bank_cntry_code	Account bank country.
tpp_bank_num	Account bank number.
tpp_bank_name	Account bank name.

Table 12 lists the fields that appear on the analyst transaction grid for Checking/Savings Account Non-monetary (CheckSavAcct > NMonAct).

Table 12. *Checking/Savings Account Non-monetary*

Column Name	Column Description
rqo_tran_date_alt	Date of the transaction for display. This value is client driven.

Column Name	Column Description
rqo_tran_time_alt	hhmmssth - Time of the transaction for display. This value is client driven.
last_rule_fired	The last rule that fired on the transaction.
all_rules_fired	All rules that fired on the transaction.
aqo_acct_num	Account number of the primary interest (for example, the transacting account for payment card transactions).
tng_tran_type	Non-monetary transaction type. For more information, see *SAS Fraud Management: Message Specification*.
tng_category	Non-monetary transaction category. Convention: B: Fulfillment initiated by the bank. F: Fulfillment based on customer's request. R: Customer's request. U: Fulfillment (source unknown).
tng_tran_status	Transaction status. Convention: R: Rejected. N: Normal.
tng_status_reason	Client-defined status reason.
tng_sub_tran_type	Client-defined sub-transaction type to indicate a specific change.
tng_eff_date	ccyymmdd - Non-monetary effective date.

Column Name	Column Description
tng_exp_date	ccyymmdd - Non-monetary expiration date.
hob_ip_address	IP address.
hob_ip_address_v6	IP address v6.
hob_ip_cntry_code	Three-digit ISO country code representing the location of the IP address.
hob_device	Online banking device type. Convention: A: Mobile phone app. C: Computer. M: Mobile phone browser.
hdf_dev_fp_val	Device fingerprint hash string.

Resources

SAS Fraud Management documentation is intended for use by existing customers and requires an access key. You can obtain the access key from your SAS consultant or by contacting SAS Technical Support. To expedite your request, please include **SAS Fraud Management** in the subject field of the form. Be sure to provide the SAS Site Number for your software license along with your request.

Release Information Content Version: 1.0 February 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