# Global Risk Investigations ("RI") Fraud Queue Review Work Instruction SOP778

Publish Date: 2023-03-28

# 1. WORK INSTRUCTION

This work instruction outlines the steps for investigating fraud queue accounts.

Accounts are queued for Risk Investigations ("RI") review when risk mitigation is needed for PayPal and customers. RI reviews and transitions RI queued accounts, including investigator resources, which are utilized as appropriate to queue, case, and risk type being worked.

## 1.1 INITIAL REVIEW

A. Obtain case via Cassini Venus

B. Determine if account holder (AH) is an employee:

- No: Continue review
- Yes: Escalate account – See *Global Risk Escalation Work Instruction (SOP786)* for assistance

C. Determine if account is currently limited:

| Limited | Limitation Type | Action |
|---|---|---|
| No | N/A | Continue review |
| Yes | CRS | 1. Review linked accounts for circumvention<br>2. Limit linked accounts – See *Global RI Limitation Placement Work Instruction (SOP1354)* for assistance<br>3. Determine if active limitation mitigates account risk:<br>▪ Yes: Restrict case<br>▪ No: Continue review |
| | Seller Risk Services (SRS) | |
| | Global Investigations (GI) | Follow instructions found in GI limitation note |
| | Other | 1. Identify additional risk indicators<br>2. Notate account accordingly<br>3. Continue review |

D. Determine if customer previously confirmed account activity:

- Activity not confirmed: Continue review
- Activity confirmed: Dismiss case

NOTE: Dismissal is permissible only if confirmed activity matches the queue reason.

E. Determine if flags present on CCI Home page:

| If… | Then… |
|---|---|
| No flags present | Continue review |
| Flags present | 1. Review Service Log for additional notes regarding flags<br>2. Follow instructions if Service Log notes present<br>3. Continue review |

F. Review Activity Log for other teammates in account:

| If… | Then… |
|---|---|
| No teammate in account | Continue review |

| | |
|---|---|
| Teammate in account | Send email to other teammate via Outlook to determine if account review occurring:<br>▪ Review occurring: Later case for one hour<br>▪ No review occurring or no response: Continue review |

## 1.2 CCI Review

Review for signs of account takeover (ATO), stolen financials, issues with linked accounts, and false identity.

A. Access CCI (via Venus or within the CCI standalone (go/cci/)

B. Identify account creation date.

C. Determine if recent IP, Visitor ID (VID), and Flash Shared Objects (FSO) are associated with risk:

| Determination | Action |
|---|---|
| No risk found | Continue review |
| Risk found | 1. Complete review of associated accounts for potential fraud and take appropriate action as needed –See *Global RI limitation Placement Work Instruction (SOP1354)* for assistance<br>2. Flag IP/VID/FSO/DID – See *Global Risk Account Identifiers Work Instruction (SOP759)* for assistance<br>3. Continue review |

D. Determine number of accounts linked to Device ID (DID)– See *Global Risk Account Identifiers Work Instruction (SOP759)* for assistance:

- 5 or less: Complete review of accounts
- 6-100: Confirm access to Hydra
  - No: Escalate queued account to Emb Spec via PET – See *Global Risk Escalation Work Instruction (SOP786)* for assistance
  - Yes: Submit Mass Restriction – See *NA RI Emb Spec Hydra Admin Tool Guide (SOP1127)* for assistance
- More than 100: Escalate queued account to Emb Spec via PET – See *Global Risk Escalation Work Instruction (SOP786)* for assistance

E. Review for additional linked account(s):

| Determination | Action |
|---|---|
| No account identified | Continue review |
| Linked account(s) identified | 1. Complete review of associated accounts for potential fraud, taking appropriate action as needed – See *Global RI limitation Placement Work Instruction (SOP1354)* for assistance<br>2. Determine if linked account affects review decision – See *Global Risk Account Linking (SOP784)* for assistance<br>3. Continue review |

F. Review following for credit card risk:

- Accounts linked by credit card

- Batch Identification Number (BIN):
  1. Copy 16-digit credit card number
  2. Open Admin Tools Bin Info tab
  3. Select *Query* via dropdown
  4. Paste 16-digit credit card number into card number field

     **NOTE:** Since BIN-checker is located on Bin Info tab in Admin Tools, it is safe to utilize 16-digit CC number. When utilizing third party BIN-checker, only first 6 digits are copied.
  5. Click **Submit**
- Card currency
- Confirmation status
- Date added to account
- Lifetime denied dollar amount
- Lifetime successful dollar amount
- Name association
- Prepaid card

G. Review following for bank account risk:

- Business association
- Confirmation status
- Date added to account
- Linked accounts
- Name association
- Prepaid bank
- Routing number

H. Review profile information for risk:

| Profile Section | Risk Indicators |
|---|---|
| Email Address | ▪ Inconsistency with name on account<br>▪ Linked accounts<br>▪ Multiple/Newly added<br>▪ Suspicious domain name<br>▪ Suspicious prefix |
| Street Address | ▪ Fraudulent/Rejected Partner flag<br>**NOTE:** If determination made that address requires flag update – See *Global RI Fraudulent Address Review and Update (SOP1067)* for assistance.<br>▪ Geographically inconsistent location<br>▪ Invalid information<br>▪ Linked accounts<br>▪ Multiple added to account from inconsistent states or locations |
| Phone Number | ▪ Area code not matching address location<br>▪ Invalid information<br>▪ Linked accounts<br>▪ VOIP phone number |
| SSN/TIN/EIN | ▪ Accounts sharing same info<br>▪ Invalid number |

| | |
|---|---|
| CPF and DOB verification (LATAM Risk) | CPF number and DOB on Receita Federal do Brazil website do not match AH details |
| **NOTE:** APAC/EMEA Risk Teammates working Collusion MO review additional risk indicators – See *Global RI Collusion Queue Work Instruction (SOP1058)* for assistance. | |

## 1.3 Transaction Log Review

Transactions are reviewed via Cassini Venus or CCI standalone (go/cci/). Identify if recent transactions are consistent with normal account activity, comparing changes in customer behavior, login, and account information to establish patterns.

A. Identify payment history:

| Activity | Review Point | |
|---|---|---|
| Bank Withdrawal | ▪ Bank name<br>▪ Date added<br>▪ Duration of funds in account | ▪ Funds transfer between financial institutions<br>▪ Withdrawal history |
| Mobile Payments | ▪ IP history to establish consistency between mobile logins<br>▪ Purchase history associated with mobile payments | |
| Personal Payments | ▪ Download Log (DLL)<br>▪ Funding source<br>▪ Memo/notes | ▪ Transaction amount<br>▪ Transaction date |
| Purchases | ▪ Average price change<br>▪ Currency mismatch<br>▪ Denied payments<br>▪ DLL<br>▪ eBay ID matches buyer information<br>▪ Frequency of payments to same counterparty<br>▪ Funding source<br>▪ Item description | ▪ Large, whole dollar payments<br>▪ Links to seller account<br>▪ Memo/notes<br>▪ Payment attempts<br>▪ Suspicious counterparty<br>▪ Transaction amount<br>▪ Transaction dates |
| Received Payments | ▪ Change in product<br>▪ High risk merchandise | ▪ Suspicious spending after payment receipt<br>▪ Transaction types |

B. Review counterparty for below indicators: Contact seller if additional information is required – See *Global RI Outbound Calling Work Instruction (SOP783)* for assistance

- Account age
- Account limitations
- DLL
- Drop shipping
- Explosive growth
- Funds movement
- High risk exit activity
- Linked accounts
- Payment consistency
- Signs of ATO
- Signs of collusion

C. Identify if counterparty risk present:

- No: Continue review
- Yes: Escalate account to SRS via PET - See *Global Risk Escalation Work Instruction (SOP786)* for assistance

D. Notate findings.

## 1.4 Service Log Review

Utilize below to complete Service Log review.

A. Navigate to CCI Service Log

B. Review for previous limitations:

| Determination | Action |
|---|---|
| Limitation(s) not present | Continue review |
| Limitation(s) present | 1. Review previous limitation(s) for following:<br>▪ Additional communication in ATTACK case<br>▪ Attached documentation<br>▪ Lifting date<br>▪ Limitation date<br>▪ Teammate notes<br>2. Consider following during review:<br>▪ Activity that caused previous limitation<br>▪ Continued account activity<br>▪ Whether limitation was lifted appropriately<br>3. Notate findings<br>4. Continue review |

C. Review previous account notes.

D. Analyze previous customer contacts.

E. Review status of claims, disputes, ACH returns, or chargebacks via ATTACK.

F. Evaluate Unauthorized Parent and Child claims if applicable – See *Global Risk Unauth ATTACK Parent Claims Work Instruction (SOP792)* and *Global Risk CG Unauth AI Review Work Instruction (SOP1906)* for assistance.

G. Notate findings.

H. Continue review.

## 1.5 Activity Log Review

Utilize below process to review CCI logs (Activity, transaction, and service log.)

A. Review following information:

- Error messages
- Failed authorization flows/validation
- IPs and VIDs
- Login times
- New financial information
- Notes by other teammates
- Profile changes
- Recent password, security questions, and/or profile changes
- Rejected credit card errors
- Transaction reversal notes

B. Notate findings

C. Continue review

## 1.6 Additional Tools

Utilize below information to complete review of additional tools.

- LexisNexis Risk Research (US accounts only) – Widget for LexisNexis Risk Research can be found in CCI.

  A. Search customer utilizing below information:

  - Address
  - Phone Number
  - Name
  - SSN

  B. Compare account information to generated results

  C. Utilize Get Person Report if necessary (NA Risk Only)

  NOTE: Get Person Reports are available at an additional fee and should only be used when necessary.

## 1.7 Review Resolution

After investigating account, associated accounts, risk indicators, and customer activity, determine if the account presents a risk to PayPal or the customer. An outbound phone call provides information not available during review – See *Global RI Outbound Calling Work Instruction (SOP783)* for assistance.

A. Determine if additional information is required:

- No: Continue review
- Yes: Later case

B. Determine if activity is illicit (e.g. money laundering, financial fraud, terrorism financing, etc.):

| If… | Then… |
|---|---|
| No | Continue review |
| Yes | 1. File Suspicious Activity Report (SAR) – See *Global ERC Jurisdictional Referrals and Quick Submit (SOP434)* for assistance<br>2. Continue review |

C. Determine if additional escalation is required:

| If… | Then… |
|---|---|
| Escalation not required | Continue review |
| Escalation required | 1. Escalate account – See *Global Risk Escalation Work Instruction (SOP786)* for assistance<br>2. Continue review |

D. Identify if account is cash advancing:

- No: Continue review
- Yes: See *Global Risk Cash Advance Review Work Instruction (SOP782)* for assistance

E. Determine if additional risk present:

| Risk Type | Action |
|---|---|
| None | Continue review |
| ATO Peek | 1. Set Peek IP flag:<br>a. Access Account-Level Flags section of CCI Home Page<br>b. Select *alf_ATO_peek_event flag* via Select Account-Level Flag dropdown<br>c. Set Expiry Date to *1 month*<br>d. Click **Set Flag**<br>2. Dismiss account |
| Fraud Risk | Determine account type:<br>▪ DCC: Lock account, ending review<br>▪ All other account types:<br>1. Reverse transactions as appropriate – See *Global Risk Transaction Reversal and AFR Placement Work Instruction (SOP781)* for assistance<br>2. Restrict account |

## 1.8 Resolve Case

Complete below steps to resolve case after risk assessment completed.

| Case Resolution | Action |
|---|---|
| Dismiss | A. Select *Resolve Case* via Take Action dropdown<br>B. Remove any Related Active Cases when applicable<br>C. Mark *Dismiss*<br>D. Enter full dismissal note including recap of review and all mitigating factors leading to dismissal<br>E. Click **Submit**<br>F. End review<br>**NOTE:** Select *Dismiss* when removing active limitations that are identified as inappropriate. |
| Later | A. Select *Later Case* via Take Action dropdown<br>B. Enter later date utilizing whole hour format<br>**NOTE:** EMEA teammates follow specific guidelines when latering accounts – See Appendix 3.1: EMEA Latering Guidelines for assistance<br>C. Enter applicable notes<br>D. Click **Submit**<br>E. End review |
| Restrict | A. Refer to *Global RI Limitation Placement Work Instruction (SOP1354)* for assistance<br>B. Resolve case as *Risk Found* within Cassini Venus<br>C. Remove any Related Active Cases when applicable<br>D. Enter detailed restriction note<br>E. Click **Submit**<br>**NOTE:** If active restriction addresses identified risk, select *Risk Found* without placing additional limitation. |
| **NOTE:** Do not include restricted information in account notation (e.g. full credit card number, full bank account number, SSN, etc). | |

## 2. TOOLS

- ATTACK
- Cassini Venus
- CCI
- Compass Gold
- KANA
- LexisNexis (NA only)
- Microsoft Office
- PET
- Receita Federal do Brazil website (Brazil only)

## 3. APPENDICES

### 3.1 EMEA LATERING GUIDELINES

Outlined below are EMEA regional guidelines for latering accounts.

| Situation | Reason Note | Later Duration |
|---|---|---|
| PET ticket created to another department (e.g. ROMs, BRM, Emb Spec, etc.) | Awaiting update on Pet ticket no XXXX | 24 hours |
| Call back request from customer | Customer asked to ring back at later time | Later until relevant time (e.g. 1/2/3 hours, etc.) |
| Language support from another teammate needed | Outbound call language support | 2 hours max |
| Authorization sent to airline merchant and need to wait for auth to capture for flight information | Airline Authorization | 24 hours |
| Teammate forgets to select unavailable before meeting, huddle, 1:1, TLS, break, lunch | Latering due to huddle, meeting, 1:1, TLS | 1 hour |
| New teammate needs assistance from tenured teammate | Awaiting tenured teammate for support on review | 1-2 hours |

## 4. DOCUMENT CONTROL

| Version | Change Summary | Process Owner | Approver(s) | Publish Date |
|---|---|---|---|---|
| 3.2 | Replaced all references to Fraud One Page (FOP) with Argus due to global tool replacement and updated to new template.<br>This published document aligns with Metapolicy requirements. Previous document versions are available upon request. | Ron Lee | Liu Lina | 20180419 |
| 3.3 | Section 5.8, Resolve Case; Dismiss, Replaced step D with new version.<br>This published document aligns with Metapolicy requirements. Previous document versions are available upon request. | Ron Lee<br>Ashley Gamblin | Vincent Zhou<br>Ron Lee<br>Ashley Gamblin | 20180516 |
| 3.4 | Updated GAP to GI and minor formatting | Ashley Gamblin | Megan Love | 20180718 |
| 3.5 | Updated template and minor formatting. This published document aligns with Policy Governance requirements. | Ashley Gamblin | Megan Love | 20190103 |
| 4.0 | Updated procedure owner; Replaced Risk Compass with Cassini Venus. | Zhao Ziqian | Lina Liu<br>Zimmerman Ryan<br>Lina Xia | 20190831 |
| 4.1 | Replaced ICA references with Embedded Specialist (Emb Spec); Section 5.2: Step C: Minor formatting updates to clarify Hydra and flag steps; Step D: Rewrote step for number of accounts linked to DID; Section 5.3: Step B: Removed Note and escalation to SRS and rewrote as Step C if counterparty risk present | Zhao Ziqian | Megan Love<br>Zhao (Steven) Ziqian<br>Wendy Muher | 20191114 |
| 4.2 | Updated template from Procedure to WI; Section 1.8: Added NOTE to table; | Zhao Ziqian | Joshua Felker<br>Carlos Rodriguez<br>Zhao Ziqian<br>Wendy Muher | 20200305 |

| | | | | |
|---|---|---|---|---|
| 4.3 | Section 1.8: Resolve Case > Under table section > Modified Note | Ziqian Zhao | Sandhya Sharma<br>Ziqian Zhao | 20200317 |
| 4.4 | Section 1.2 Argus Review, Step C, Risk Found Steps 1 and 2: Updated guidance for actions taken when risk identified; Section 1.2 Argus Review, Step E, Linked account(s) identified Step 1: Updated guidance for actions taken when linked account(s) identified | Ziqian Zhao | Sandhya Sharma<br>Ziqian Zhao<br>Jessica Kirkpatrick<br>Wendy Muher | 20200629 |
| 4.5 | Section 1.3 > Step B > Updated name of SOP referenced to Global CRS Outbound Calling Work Instruction; Section 1.7> Replaced reference to Global CRS SFO Outbound Calling (SOP1624) with Global CRS Outbound Calling Work Instruction (SOP783) | Ziqian Zhao | Megan Gillam<br>Megan ORourke | 20210409 |
| 5 | Off-cycle Material Update: Section 1.1 > Initial Review > Updated with new guidance; Section 1.2 > CCI Review > Updated with new guidance; Section 1.3 > Transaction Log Review > Updated with new guidance; Section 1.5 > Activity Log Review > Updated with new guidance; Section 1.5 > Additional tools > Updated with new guidance. | Ziqian Zhao | Ryan Zimmerman | 20230328 |