**Green Dot**

**Lookback Case Review Investigation (“Lookback”) and Quality Control (“QC”) Procedures**

June 2025

V1.3

*Procedures subject to change based on Lookback Pilot*

Table of Contents

[**1.** **Introduction** 8](#_Toc200364613)

[**1.1.** **Background** 8](#_Toc200364614)

[**2.** **Case Review Investigation Overview** 8](#_Toc200364615)

[**2.1.** **Project Overview** 8](#_Toc200364616)

[**2.1.1.** **Phase 1: Identification of Alerts and Cases for Investigation** 8](#_Toc200364617)

[**2.1.2.** **Phase 2: Lookback Review** 8](#_Toc200364618)

[**2.1.3.** **Phase 3: Final Report** 9](#_Toc200364619)

[**3.** **Case Review Investigation Roles and Responsibilities** 9](#_Toc200364620)

[**3.1.** **Case Investigation Team** 9](#_Toc200364621)

[**3.1.1.** **Investigators:** 9](#_Toc200364622)

[**3.1.2.** **Quality Control (QC) Analysts:** 10](#_Toc200364623)

[**3.1.3.** **Team Leads:** 10](#_Toc200364624)

[**3.1.4.** **Schedulers:** 10](#_Toc200364625)

[**3.1.5.** **Lookback Senior Management:** 11](#_Toc200364626)

[**3.1.6.** **Green** **Dot Senior Management** 11](#_Toc200364627)

[**4.** **Case Review Investigation Procedures** 11](#_Toc200364628)

[**4.1.** **Case Assignment and Selection** 11](#_Toc200364629)

[**4.2.** **Case Investigation** 11](#_Toc200364630)

[**4.2.1.** **Log into ECM and Identify Assigned ECM Focal Entity(ies) Cases** 11](#_Toc200364631)

[**4.2.2.** **Review the Scope of the Case in ECM** 11](#_Toc200364632)

[**4.2.3.** **Download and Save the Alerted Transaction File** 13](#_Toc200364633)

[**4.2.4 Review the Alerted Transaction File** 14](#_Toc200364634)

[**4.2.5** **Conduct Due Diligence and Review Adverse News Screening on the Focal Entity(ies)** 16](#_Toc200364635)

[**4.2.6** **Conduct Due Diligence and Review Adverse News Screening on Counterparties** 18](#_Toc200364636)

[**4.2.7** **Conduct Office of Foreign Asset Control (OFAC) sanctions screening on the Focal Entity and sampled counterparties** 19](#_Toc200364637)

[**4.2.8** **Complete the Alert Disposition** 20](#_Toc200364638)

[**4.2.9** **Review Case Narrative** 20](#_Toc200364639)

[**4.2.10** **Attach Supporting Documentation** 20](#_Toc200364640)

[**4.2.11** **Promote the Focal Entity(ies) Case to QC:** 21](#_Toc200364641)

[**4.2.12** **Promote the Focal Entity(ies) Case to Issue Management** 21](#_Toc200364642)

[**5.** **Quality Control Procedures** 22](#_Toc200364643)

[**5.1** **QC 1 (Offshore):** The QC 1 Analyst (QC Analyst) is responsible for the preliminary evaluation of the cases completed by Investigators, regardless of the alert classification recommended by the Investigator. 22](#_Toc200364644)

[**6. Case Referral to Green Dot and Closing Cases with Potential Suspicious Activity** 26](#_Toc200364645)

[**6.1 Escalation to SAR:** In the event that potential suspicious activity is identified, the Case will be referred to Green Dot Senior Management for review and determination of whether a SAR will be filed 26](#_Toc200364646)

[**Appendices** 27](#_Toc200364647)

[**Appendix A: Transaction Monitoring Rules** 27](#_Toc200364648)

[**Appendix B: Common Transaction Monitoring Red Flags** 29](#_Toc200364649)

[**Appendix C: Common Definitions** 29](#_Toc200364650)

[**Appendix D: High Risk Countries** 30](#_Toc200364651)

[**Appendix E: Case Narratives** 33](#_Toc200364775)

1. **Introduction**
   1. **Background**

Green Dot Bank (“Green Dot”) engaged Deloitte Transactions and Business Analytics LLP (“DTBA”) as an independent third-party to assess whether suspicious activity involving high-risk customers or transactions at, by or through the bank were identified and reported in accordance with DTBA’s understanding of applicable suspicious activity reporting (“SAR”) regulatory requirements.

1. **Case Review Investigation Overview**
   1. **Project Overview**

DTBA will perform a Transaction Monitoring Lookback (the “Lookback”) using a three-phased approach. DTBA completed Phase 1 in May 2025 and is submitting the scope and rules to the Federal Reserve Bank (“FRB”) prior to starting the case investigations in Phase 2.

* + 1. **Phase 1: Identification of Alerts and Cases for Investigation**

1. For background, the objective of Phase 1 of the project was to create a lookback environment, apply rules, and develop investigation protocols. The following activities were engaged to meet this objective:
   1. Receive Transactions for the covered period from Green Dot, standardize and load the data into DTBA’s technical environment
   2. Assess Green Dot’s products against red flags/typologies from regulatory and industry sources for applicability
   3. Develop rules based on applicable red flags
   4. Apply rules to in-scope activity to generate alerts and create customer-account based cases
   5. Load cases into DTBA’s Enterprise Case Manager (“ECM”) tool customized for the Lookback
   6. Create Lookback and quality control procedures, investigation protocols, and training
   7. Submit rules, alerts and customer cases to FRB for non-objection
2. Phase 1 of the Lookback was completed as of May 2025.
   * 1. **Phase 2: Lookback Review**
        1. The objective of Phase 2 of the Lookback is to investigate cases to identify potentially suspicious activity using ECM. The following activities will be ongoing to fulfill this objective:
   1. Investigate cases generated in Phase 1 in accordance with investigation protocols and procedures
   2. Disposition cases as no further action or potentially suspicious (escalation)
   3. Conduct quality control review activities to monitor adherence to protocols and soundness of case dispositions
   4. Escalate potentially suspicious cases to Green Dot for SAR consideration
      1. **Phase 3: Final Report**
         1. The third phase of the Lookback will be the conclusion of the project. The objective is to complete the final Lookback report detailing the results of the Lookback.
         2. The final report will include:
            1. The methodology used to generate alerts and cases and conduct the Lookback
            2. Investigation results, including a breakdown of no further action cases and cases escalated to Green Dot for SAR consideration
            3. An assessment of cases recommend for escalation including common red flags, typologies and rule instances.
         3. The drafted final report will be shared with Green Dot and the FRB, wherein it will be updated based on feedback received from Green Dot (limited to factual accuracy)
         4. The final report will be submitted to the regulators
3. **Case Review Investigation Roles and Responsibilities**
   1. **Case Investigation Team**

The Lookback Case Investigation Team is comprised of Investigators, Quality Control Analysts, Team Leads, Schedulers, Deloitte Senior Management, and the Green Dot SAR Team. The responsibilities of each these roles is described below.

* + 1. **Investigators:**
       1. The Investigator’s role functions within Phase 2 of the Lookback to analyze alerted activity, identify the transacting parties, determine if the activity appears suspicious or not, and then disposition the case by either recommending escalation of suspicious activity further for SAR filing, or recommending that the case be closed as not suspicious.
       2. Investigators are responsible for conducting Level 1 reviews of cases generated in Phase 1 in accordance with investigation protocols and procedures, as outlined in this document. A high-level overview of the Investigator’s activities is as follows:
          1. Conduct initial alert review triage to determine whether the rule is valid and if the investigation should proceed

If the alert is deemed a potential false positive, the Investigator is responsible for moving the case to the Issue Management queue for Team Lead review

* + - * 1. Conduct a review of Alerts and Alerted Transactions
        2. Conduct Due Diligence on Focal Entities and Counterparties
        3. Disposition alerts
        4. Upload supporting documentation
        5. Compose the final case narrative
    1. **Quality Control (QC) Analysts:**
       1. The QC Analyst’s role takes effect in Phase 2 of the Lookback to review cases dispositioned by Investigators.
       2. There are two levels of QC:
          1. QC1 (generally offshore) conducts a review of all cases (escalated and non-escalated)
          2. QC2 will conduct a second review of all cases, and is responsible for closing out the cases following completion of the procedures
       3. The QC Analyst is responsible for reviewing the case after the Investigator has completed their review and dispositioned the case. The QC Analyst’s review should confirm that the Investigator complied with the Lookback Procedures, and appropriately investigated, dispositioned, and documented their decision on the case. QC Analysts, at a high-level, are responsible for reviewing the following:
          1. The validity of each alert for the case has been analyzed and confirmed (i.e., an alert was not a false positive)
          2. Due diligence was properly conducted on the Focal Entity and Counterparties
          3. Alerted transactions were properly analyzed with consideration of transaction patterns, account history, and red flags
          4. The documentation recorded in ECM is accurate and comprehensive
          5. The conclusion reached by the Investigator is appropriate and aptly documented in the alert closure/alert referral form
          6. Alert disposition(s) and the rationale for determining whether the alert was suspicious or not suspicious were suitably provided
          7. The generated Case Narrative is accurate and aligns with investigation findings
    2. **Team Leads:** 
       1. The Team Leads’ role within Phase 2 of the Lookback is to oversee the investigations process.
       2. The Team Leads are responsible for:
          1. Issue Management queue review and response (answering questions or escalating cases further for potential Green Dot team review)
          2. Escalating any unresolved Issues to Lookback Senior Management
    3. **Schedulers:**
       1. The primary responsibility of the Schedulers is to manage the daily assignment of cases to team members, ensuring an even distribution of workload and timely processing. In addition to assigning cases, Schedulers closely monitor the aging of cases across various levels to track progress and identify cases that may require immediate attention.
    4. **Lookback Senior Management:**
       1. Deloitte Senior Management’s role is to oversee the Lookback project. Within Phase 2 of the Lookback, the Lookback Senior Management (or their delegates) will:
          1. Assist and act as the point of escalation for any Issue Management issues raised by the Team Lead
          2. Present all cases in which potential suspicious activity has been identified to the Green Dot Senior Management
    5. **Green** **Dot Senior Management**
       1. The Green Dot SAR Team includes executives from Green Dot’s Suspicious Activity FIU
       2. The Green Dot SAR Team is responsible for reviewing cases recommended for SAR filing, determining whether Green Dot agrees with the recommendation, and conducting SAR filing requirements, per Green Dot policies and procedures

1. **Case Review Investigation Procedures**
   1. **Case Assignment and Selection**

In order to initiate the review of a case, the Scheduler (or designee) will assign cases to investigators through ECM.

Cases are organized around Focal Entities and rules that are triggered by the transaction activity for the Focal Entity(ies) (Alerts). Each Case includes Alerts associated with the Focal Entity(ies) for the Lookback Review Period.

* 1. **Case Investigation**
     1. **Log into ECM and Identify Assigned ECM Focal Entity(ies) Cases**

1. Investigator will log into ECM using their assigned credentials in the ECM PROD POOL Desktop
2. Once logged in, the Investigator will identify their Cases and choose the highest priority Case to work on first by clicking on the Focal Entity(ies) case hyperlink.
3. Upon opening, the Case will move into “In-Progress”
   * 1. **Review the Scope of the Case in ECM**
4. Once the Investigator has opened the Focal Entity(ies)’s case in ECM, the Investigator will find the following tabs within the Focal Entity(ies) case:
   1. Statistics
      * Account Details: Accounts affiliated with the Focal Entity(ies) for any alerted activity and CIP data (Product, customer address, DOB, email, phone #)
      * Alerts Summary: Summary of the rules and alerts including the rule name, rule definition, alert IDs, transaction count, date range, and total dollar amount per alert.
      * Focal Entity Summary: summary of total transaction activity and total transaction volume for the alerting activity for the Focal Entity
      * Lookback Transactions Summary: Summary of the Lookback alerting transaction including the number of counterparties, products used, sum and count of credits and debits, etc.
      * Lookback Period Data: Summary of the Lookback activity via bar graph
   2. Requirements – The following sections will then appear:
      * Counterparty Selection: Fields to input Counterparties selected for due diligence based on alert review (see Section 4.2.3.i for counterparty selection details), etc.
   * Counterparty names should be separated by semicolon (no space should be included)
   * Various well-know merchants that process GD transactions are not considered valid for counterparty selection.[[1]](#footnote-2) Normal counterparty documentation procedures are not required if it is a well-known entity.
     + Due Diligence:
   * Fields to input Focal Entity name(s), [[2]](#footnote-3) alerting rules, Focal Entity(ies)’s location, available space to provide information on each Focal Entity(ies)’s occupation/nature of business, a summary of screening results, etc.
   * Counterparty Due Diligence
   * Fields to input names of each selected Counterparty (see Section 4.2.4), each Counterparty’s location, available space to provide information on each Counterparty’s occupation/nature of business, a summary of screening results.
     + Alert Review: Rule violated, total transaction count, total amount, date range, alert disposition, rationale for the alert disposition, etc.
     + Case Review: Alerted rules, alerted rule count, final case disposition, and generated case narrative based on inputs from previous tabs
5. In the Statistics tab, the Investigator will review the Focal Entity(ies) Information, including the following:
6. Account Details and note any details that may indicate potential suspicious activity or red flags
   * + Account Number(s)
     + Account Type(s)
     + Product Type(s)
     + Account Status(es) [[3]](#footnote-4)
7. Focal Entity(ies) CIP Information for each account and note any variances that may indicate potential suspicious activity [[4]](#footnote-5)
   * + Name
     + Address
     + Date of Birth (DOB)
     + Email
     + Phone Number
8. The Investigator will review the Alerts Summary table (located in the Statistics tab) for an overview of each alert’s activity including the following:
   * + Rule(s)
     + Rule Definition(s)
     + Alert ID(s)
     + Transaction Count
     + Date Range
     + Total Amount for alerted activity
9. The Investigator will review the Lookback Transaction Summary table and Lookback Period Data for an overview of the 15-month Lookback activity including the following:
   * + Number of Counterparties
     + Total Volume and Amount of Debits
     + Total Volume and Amount of Credits
     + Products the Focal Entity(ies) utilized
     + Alerted Transaction Date Range (First and Last Alerted Transaction Dates)
     + Minimum, Maximum, and Average Transaction Amounts
     + Utilize the dropdown for Account # to see the historical transaction summary table per account #
     + Any spikes in activity during the review period (volume, frequency, dollar amounts, number of counterparties, etc.)
     + The types of transactions the Focal Entity(ies) has carried out and if they appear in certain months
     1. **Download and Save the Alerted Transaction File** 
        1. In the Statistics tab, under the Alerts Summary, the Investigator will click “Download Alerted Transactions Table” to download the alerts transaction table[[5]](#footnote-6).
10. A new tab will open with the data and the Investigator will click the export dropdown menu and download it to excel. Upon downloading, a macro will automatically run that will provide a tab in the Alerted Transaction File:
    * + 1. Alerted Transactions – which will show a column for each rule that hit and the alert ID in the applicable transaction rows
11. Upon opening the Alerts Transaction File, the investigator will:

Sort “Date” by oldest to newest

Color code all credit rows in green and all debit rows in red.

1. In addition to the Alerted Transaction File, the Investigator will click in the Statistics Tab of ECM under Alerts Summary the “Download Counter Party Details” to download the file which will show the list of Counterparty Details associated with the alerted transactions

**4.2.4 Review the Alerted Transaction File**

1. In the Alerted Transactions File, the Investigator will conduct a high-level review of the Focal Entity(ies)’s alerted transaction activity, and take note of the following:
2. The time frame (for example, does the Focal Entity(ies) alert across the entire 15-month Lookback Period or just for a particular period)
3. If alerted activity spans multiple accounts and products, noting whether the product is associated with a Small and Medium-size Business (“SMB”) or consumer
4. The transactions occur outside of the United States (“US”) – *Note: Green Dot does not identify countries in their transaction file – if there is no State in the “Counterparty\_State” column, this means that the counterparty is likely outside the US. The investigator will need research, based on city, which country the counterparty is located. If the country cannot be determined, the Investigator should move the Case to Issue Management for TL review.* 
   * + If any transaction(s) occurs outside of the US, please reference Appendix E to see if the country is listed as a High-Risk Jurisdictions
5. In many cases, the alerted transactions should provide the Investigator with the ability to understand the source and use of funds, however if additional transactions are needed, the Investigator will navigate to the Statistics Page and download the 15-month transaction history from “Download Historic Transaction Table” under Lookback Period Data.
6. Compare the Focal Entity(ies)’s alerting transactions to the Lookback Transaction Summary and Lookback Period Data [[6]](#footnote-7) in the Case Overview tab in ECM, noting any potential differences from the 15-month behavior.
7. Review each alert (based on Alert ID) in the Alerted Transaction File:
   1. To properly filter on each alert, the Investigator will filter by Alert Id under the respective rule starting in column B. For example, if Alert ID 12345 is associated with Rapid Movement of Funds, the Investigator should filter using that Alert ID on the Rapid Movement of Funds column.
   2. The Investigator will first determine whether the alert is valid by comparing the alert to the definition of the rule and rule thresholds
      * If the alert is a potential false positive [[7]](#footnote-8), in the Alert Review tab (under Requirements in ECM), the Alert ID should be marked as “False Positive,” an Alert Disposition Rationale selected, and a description of the reason for the determination added in “Analyst Comments.” Upon selection, the entire Case should be moved to the Issue Management queue for review by a Team Lead (see Section 4.2.12 for details on Issue Management).
      * If all of the alerts are valid, continue with the review
   3. The Investigator will conduct an initial review of the transactions associated with each Alert:
      * Based on the product(s) listed in the “Product” column associated with the alerted accounts, review the Green Dot Product Training and Guide to understand:
8. Description of the product
9. The product transaction limits (e.g., daily cash limit, MoneyPak limit)
10. Potential money laundering risks and red flags
    * + Identify the timeframe and order of transactions (Transaction Date column)[[8]](#footnote-9)
      + Determine whether additional transactions are needed to understand the source or use of funds.[[9]](#footnote-10)
11. The Investigator will select Counterparty(ies) for review:
12. Using the Alerts Transaction Table Excel and Counter Party Details Excel, select a minimum of one valid counterparty[[10]](#footnote-11) for review, per alert:
    * + - A valid counterparty would be an individual or SMB that is engaged in the activity and represents the alert
        - Major, well-known entities,[[11]](#footnote-12) such as Walmart or a bank, would not be considered valid for the purposes of the Lookback
        - In some instances, the transaction data indicates that the counterparty is actually an activity descriptor (e.g., Cash App\*Cash Out), which would not be considered a valid counterparty
      + A counterparty may be selected to cover multiple alerts if deemed to impactfully represent the various alerts the counterparty is selected for, as well as the potentially unusual activity
13. Enter all counterparties in the String Search Excel file (note, you must be in the ECM CORP POOL). If known, the city and zip code should be included.[[12]](#footnote-13)
14. Save the file in the Investigator’s Z: Drive file
15. Once counterparties have been selected, if applicable, the Investigator will click the “Run” button-
16. A bot will run Google string search on the selected counterparties and save the file(s) in the Investigator’s Z: Drive file.[[13]](#footnote-14) See step 4.2.6 for counterparty screening process.[[14]](#footnote-15)
17. In the Requirements tab – under Counterparty Selection in ECM, the Investigator will copy and paste the names of all counterparties that were subject to screening based on step 4.e (,Counterparty names should be separated by semicolon and no space), check “Populate Counterparty Due Diligence details,” and click “save requirements.”
    1. A PDF is not required for every counterparty/counterparties unless there is related adverse media found.
       1. **Conduct Due Diligence and Review Adverse News Screening on the Focal Entity(ies)**
18. In the Requirements tab - Due Diligence section in ECM, the Investigator will navigate to the Focal Entity Due diligence section:
19. The Investigator will review the focal entity(ies) CIP information (from the Statistics tab Account Details), including DOB, address, and name variations across accounts
    * + If CIP information varies across the Focal Entity(ies)’s accounts (e.g., different DOBs, addresses), please be sure to consider all CIP information when conducting screening and research on the Focal Entity(ies)
      + When searching please include the Focal entity in quotes (e.g. “John Smith”)
20. In ECM CORP POOL Desktop, Utilizing Google Search, the Investigator will conduct Due Diligence on the Focal Entity(ies), including into their occupation (for individuals) / nature of business (for entities):
    1. Print Screen for all websites used for due-diligence and save the files as “[Focal Entity Name]\_Due Diligence\_[Description]\_[DD.MM.YYYY]
    2. Record results in the Focal Entity Due Diligence (Requirements tab - Due Diligence) under “Focal Entity Occupation / Nature of Business” utilizing the industry and selecting the most applicable industry and in the Focal Entity “Additional Information” section (note: this should be in sentence form).
    3. Include additional detail, as needed, in the corresponding free text field
    4. All due diligence should be saved in the investigator’s Z:Drive folder in order to be uploaded into ECM on the ECM PROD POOL Desktop
21. The Investigator will download LexisNexis screening results (PDF), found in XXXX.
22. Upon downloading, the Investigator will review all results with 85% or above. Use the following factors to determine if an entry is a potential true match or false positive:
    * + Material name mismatch
      + Different DOB/age (plus or minus more than one year)
      + Domicile/citizenship mismatch
      + Different family information
      + Tax ID/passport number mismatch
23. A true match is generally one where there is a name match in addition to DOB/age.
24. A true match can also be determined if there is a name match and a match with any two of the following factors: nationality, geographic jurisdiction, or employment.
25. Based on the review, the Investigator will disposition each potential match in the PDF with a text box to evidence that the results were reviewed
    * + Write ups for False positives should include the mitigation factors and reference any supporting documentation
      + If a true match is identified, but activity is not considered to be adverse, write-ups should include the reason for why the news is not concerning.[[15]](#footnote-16)
      + If a true match is identified and the news/information is considered adverse (e.g., money laundering/financial crime offenses), write-ups should include indicating that the news is considered adverse and documented as part of the Case.[[16]](#footnote-17)
26. The Investigator will save the LexisNexis file with dispositions as “[LexisNexis Search Results (Document Description)\_Focal Entity Name\_ \_[MM.DD.YYYY].
27. Upon reviewing applicable screening results for the Focal Entities, the Investigator will provide summary disposition in “Focal Entity Screening Results” (e.g., true match, false positive)
    1. If a true match is identified, include a description of the adverse media in the “Focal Entity Screening Summary”
       1. **Conduct Due Diligence and Review Adverse News Screening on Counterparties**
28. Based on the counterparties selected in the Counterparty Selection section, each counterparty should have its own entry under “Counterparty Due Diligence.” For each counterparty:
29. Utilizing Google (in ECM CORP POOL), the Investigator will conduct Due Diligence on the Counterparty(ies), including into their occupation (for individuals) / nature of business (for entities)
    * + Print Screen for all websites used for due-diligence and save the files as “Due Diligence\_[Description]\_ [Counterparty Name]\_ [MM.DD.YYYY]
      + Record results in the Counterparty Due Diligence under “Counterparty Occupation / Nature of Business” and selecting the most applicable NAICS code
      + Include additional detail, as needed, in the corresponding free text field
      + In searches, please include Counterparties in quotes (e.g. “John Smith”)
30. Complete the counterparty’s geographic information (as available). Note that addresses can be identified in the transaction file, but since its’ a Lookback, the information may be out of date / not align with addresses identified through online due diligence.
31. The Investigator will download the Google String Search results (PDF), found in the Z Drive folder or where the PDF is saved.
32. Upon downloading, the Investigator will review all results. Use the following factors to determine if an entry is a potential true match or false positive:
    * + Material name mismatch
      + Different DOB/age (plus or minus more than one year)
      + Domicile/citizenship mismatch
      + Different family information
      + Tax ID/passport number mismatch

A true match is generally one where there is a name match in addition to DOB/age. A true match can also be determined if there is a name match and a match with any two of the following factors: nationality, geographic jurisdiction, or employment.

1. Based on the review, the Investigator will disposition each potential match in the PDF with a text box to evidence that the results were reviewed
   * + Write ups for False positives should include the mitigation factors and reference any supporting documentation
     + If a true match is identified, but activity is not considered to be adverse, write-ups should include the reason for why the news is not concerning.[[17]](#footnote-18)
     + If a true match is identified and the news/information is considered adverse (e.g., money laundering/financial crime offenses), write-ups should include indicating that the news is considered adverse and documented as part of the Case.[[18]](#footnote-19)
2. The Investigator will save the PDF with dispositions as [Google Screening Results \_Counterparty Name]\_[MM.DD.YYYY]
3. Upon reviewing applicable screening results for the Counterparty(ies), provide summary disposition in “Counterparty Screening Results” (e.g., true match, false positive)
   1. If a true match is identified, include a description of the adverse media in the “Counterparty Screening Summary”
      1. **Conduct Office of Foreign Asset Control (OFAC) sanctions screening on the Focal Entity and sampled counterparties**
         1. The Investigator will open up an internet search browser and access the OFAC Sanctions List Search tool (<https://sanctionssearch.ofac.treas.gov/>).
         2. Upon navigating to the website, the Investigator will:
            1. Set the minimum name score indicator to 90%
            2. Ensure that type, program, country, and list, are set to the default setting of “All.”
            3. Input the name of the focal entity or counterparty in the Name field
            4. Click the search button
            5. Save the results page as a PDF, by using print to PDF
            6. Save the screening results as [OFAC Screening Results\_Focal Entity/Counterparty Name]\_[MM.DD.YYYY]
         3. If the search does not produce results, the Investigator will repeat the process for the remaining focal entity or sampled counterparties. **NOTE: the minimum name score indicator must be reset to 90% after each search that produces results. It defaults to 100**%
         4. If there are results where the “score” column list a percentage of 90% or above, click on the hyperlink for the profile of the result
            1. Save the profile of the results page as a PDF, using print to PDF[[19]](#footnote-20)
            2. Review the information in the details page for the result, to determine whether the focal entity name is a match to the entity name
            3. Review the aliases section to determine if the focal entity name is a match to any of the aliases listed within the details page
            4. If the focal entity name is a match to the result name or an alias name, the result is a potential hit and should be escalated to a Team Lead for further review via the Issue Management queue
            5. If the focal entity name does not match the result name or an alias name, disposition the result as a non-match due to name mismatch (include a text box in the PDF).
            6. Save the screening results as [OFAC Screening Results\_ Focal Entity/Counterparty Name]\_[MM.DD.YYYY]
         5. Repeat the search for each additional focal entity or researched counterparty **NOTE: the minimum name score indicator must be reset to 90% after each search that produces results. It defaults to 100**%
      2. **Complete the Alert Disposition**
4. In the Requirements tab - Alert Review, for each Alert:
5. Based on the transaction review (see step 4.d), focal entity and counterparty due diligence and screening (see steps 5 and 6), determine if the activity should be dispositioned as, “suspicious”, “not suspicious”, or “false positive”
6. Based on the determination of suspicious or not suspicious, select the applicable reason(s) for the determination (*note: at least one reason must be selected in order to progress*).
7. Include additional commentary / details in Alert Notes
8. Upon review and disposition of all alerts, click “generate case narrative”
   * 1. **Review Case Narrative**
9. In the Requirements tab - Case Review, review the case disposition (note, if any alert has been deemed suspicious in Step 7.a, the Case Disposition will automatically be considered “Escalation Recommended”
10. Review the generated narrative, verifying the information is correct
11. Additional relevant information should be included as necessary (including any additional due diligence that may be helpful to explain the suspicious / non-suspicious activity)
    * 1. **Attach Supporting Documentation**
12. The Investigator will upload the following documents to ECM:
    1. Alerted Transaction File to ECM (see section 4.2.9 below for additional details on uploading supporting documents to the Focal Entity(ies) case in ECM)
    2. Focal Entity Screening Results
    3. Focal Entity OFAC Screening Results
    4. Focal Entity Due Diligence
    5. Counterparty Screening Results
    6. Counterparty OFAC Screening Results
    7. Counterparty Due Diligence
13. In order to upload documents, the Investigator should:
    1. Click on view attachments at the top of any ECM Case landing page
    2. Select the type of document that is being uploaded
    3. Click Choose Files
    4. Upload the respective file to the folder
       1. **Promote the Focal Entity(ies) Case to QC:**
14. Once the Case narrative has been completed and all documents have been uploaded, the Investigator will move the case to QC in ECM
    1. Go to Requirement Page and click the L1 QC circle
    2. Choose to promote the case to L1 QC – “Escalation Review Pending” or “Non-Esc Review Pending”
15. If QC1 or 2 returns the case for rework (see section 5), the Analyst should review the case fully and update based on QC comments (note a change in one section may have effects on other sections, so the Investigator should review the entire case upon return to help achieve consistency across the entire review).
    * 1. **Promote the Focal Entity(ies) Case to Issue Management**
16. If issues are identified with the case, including but not limited to the following, the Investigator should move the Case to the Issue Management queue for review by a Team Lead:
    1. Additional information from Green Dot
    2. Determination of a False Positive alert
    3. Information in ECM is incomplete
17. If an investigator determines that a case should be moved to the issue management queue:
    1. They should enter an explanatory note in the View Notes Section. Notes should be complete sentences and provide enough detail for the TL to under
    2. Go to the Requirements Page and Workflow Movement
    3. Click on the L1 Team Lead circle
    4. Choose to promote the case to “Issue Review Pending”
18. The L1 Team Lead will review the issue and add notes based on their review.
    1. If additional time is needed to review (e.g., discuss with L1 management), the case should be moved to On-Hold (under “L1 Team Lead”)
    2. Upon resolution, the L1 Team Lead will return the case by choosing “Returned- Issue Resolved” (under L1 “Team Lead”)
19. If additional guidance is needed from management or an issue needs to be opined by Green Dot, the Case should be moved to L2 Team Lead by adding additional notes and moving the case in New Summary Status to L2 Team Lead
    1. The L2 Team Lead should review. If additional time is needed to discuss with Management, the case should be moved to On-Hold. If a response is pending Green Dot, then the case should be moved to Awaiting GD Response
    2. Upon completion, the L2 Team Lead should return to the L1 Analyst (“Returned – Issue Resolved)
20. **Quality Control Procedures**
    1. **QC 1 (Offshore):** The QC 1 Analyst (QC Analyst) is responsible for the preliminary evaluation of the cases completed by Investigators, regardless of the alert classification recommended by the Investigator.

For each assigned case, the QC Analyst:

1. Logs into ECM and identifies cases that are ready for QC Analysis. These Cases are identified by the status descriptions:
   1. Not Suspicious - Assigned, but unopened
   2. Potentially Suspicious - Assigned, but unopened
2. Selects and opens a case:
   1. The QC 2 Analyst prioritizes selection of new cases based on the following order of status descriptions:
      * Potentially Suspicious
      * Close Case
   2. Within each category, prioritize alerts which have been in process the longest.
3. Once opened, the case sub-status description changes from ***“Assigned but unopened”*** to ***“In Progress.”.***
4. Conducts the QC evaluation. All feedback is provided and evaluated based on Lookback and QC Procedures and including:
   1. The validity of each alert for the case was analyzed and confirmed (i.e., an alert was not a false positive)
   2. The Focal Entity, Counterparty(ies) research, and screening performed and documented
   3. The transaction analysis that was performed
   4. The conclusion reached and documented by the Investigator in the alert closure/alert referral form
   5. Investigator’s compliance with the Lookback and QC Procedures
5. If feedback is identified, QC1 should check “Analyst Correction Required” and add an explanation of what is required to be changed in “QC Comments.”
6. Reviews the Alerted Transaction File. In performing the assessment, consideration is given to identification and documentation of appropriate transaction patterns, account history, red flags, False Positives and explainable closes, Alerted Transaction File, Investigator notes and comments.
   1. QC Analysts should identify the Focal Entities and Counterparty(ies) involved and determine if any additional counterparties should be selected based on the activity.
7. Reviews the Due Diligence tab in ECM to determine that all Focal Entities and applicable Counterparty(ies) have been subject to sufficient screening and due diligence. In performing the assessment for each Focal Entity and Counterparty, consideration is given to:
   1. The Focal Entity / Counterparty geographic location (City and State) appears to be accurate based on account / CIP information for Focal Entities, and information in the transaction file for Counterparties
   2. The Focal Entity / Counterparty Entity Status and Industry / Nature of Business appear accurate based on due diligence and information on file
   3. Focal Entity / Counterparty Screening Results are accurate and align to the documentation saved in ECM (see 5.1.vii.b and 5.1.vii.c)
   4. For Focal Entities that have been marked as duplicates / also known as, whether this designation is correct
8. Reads and assesses the documentation in ECM for the accuracy and comprehensiveness of the research performed on both the Focal Entity and Counterparty(ies) and the documentation of findings. In performing the assessment, consideration is given to:
   1. Comprehensiveness of the research performed on the Focal Entities and Counterparties
   2. Accuracy of dispositioning the OFAC search and adequate information provided to determine if any potential matches were false positives
   3. Analysis of adverse news for agreement on the relevance of materiality and age of the adverse event (i.e., although the adverse news may be old it may still be relevant due to the nature of the adverse news)
   4. Clarity and thoroughness of the documentation regarding research findings
9. Reviews each Alert disposition (Alert Review), considering the Rule Violations Transaction Excel and the documentation on Focal Entities and Counterparties (e.g., screening results). In performing the assessment, consideration is given to:
   1. Counterparty Screening: At least one counterparty was screened for each alert, and if, based on review of the Rule Violation Transaction Excel, additional counterparties should be subject to screening.
   2. The alert disposition and the rationale for determining whether the alert was suspicious / not suspicious
10. Reads and assesses the Case Narrative for accuracy and alignment with information in the Alert. QC Analysts will review and document required edits as necessary. Feedback may be focused on:
    1. Case Disposition aligns with the dispositions in Alert Review (see 5.1.viii)
    2. Overall compliance with Lookback Procedures including all required elements identified by the respective instructions and templates
    3. Any missing information as identified based on assessment of supporting documentation in the ECM
    4. Overall clarity and readability, and any inconsistencies based on research conducted, supporting documentation, as applicable
11. Completes the QC 1 Checklist, attesting that all tabs have been reviewed and feedback has been added to the QC sections.
12. Determines whether the QC Analyst agrees with the Investigator’s Case classification based on the transaction analysis, the research conducted and supporting documentation compiled. The QC Analyst has three options for dispositioning an alert:
    1. Return the Case to the Investigator for rework ensuring that feedback is included in the QC feedback boxes in each tab. Select Returned – Revisions Required in the ECM workflow to move the case back to the Investigator for rework.
    2. Accept the Investigator’s recommendation to close the alert as not suspicious. Select “Non Esc - Review Pending” in the ECM workflow to move the Case to QC 2 for final review.
    3. Escalate the Case to QC 2 for evaluation of a referral to GD for potentially suspicious activity. Select “Escalation - Review Pending” in the ECM workflow to move the Case to QC 2 for final review.

**5.2 QC 2 (Onshore):** The QC 2 Analyst is responsible for conducting a second and final quality control review on the case before either closing the case (not suspicious) and recording the final disposition, or escalating the case to Green Dot FIU for review of the SAR recommendation. The Green Dot FIU will conduct a review to determine if the SAR recommendation is appropriate and, if so, will proceed to file the SAR.

For each assigned case, the QC 2 Analyst:

1. Logs into the ECM and identifies cases that are ready for QC 2 Analysis. These alerts are identified by the status descriptions:
2. Not Suspicious - Assigned, but unopened
3. Potentially Suspicious - Assigned, but unopened
4. Selects and opens a case:
5. The QC 2 Analyst prioritizes selection of new cases based on the following order of status descriptions:
   * + Potentially Suspicious
     + Close Case
6. Within each category, prioritize alerts which have been in process the longest.
7. Once selected, the alert sub-status description changes from “Assigned but unopened” to “In Progress”.
8. QC 2 Analysts will conduct the same review as the QC 1 Analysts with respect to review of the focal entity screening, counterparty selection and screening, transaction analysis, case documentation, alert disposition, and overall compliance with Lookback Procedures, and provide feedback if necessary. See 5.1 for detailed steps.
9. If feedback is identified, QC1 should check “Analyst Correction Required” and add an explanation of what is required to be changed in “QC Comments.”
10. At a high-level, QC 2 Analysts will evaluate:

* The validity of each alert for the case was analyzed and confirmed (i.e., an alert was not a false positive)
* Due diligence was properly conducted on the Focal Entity and all relevant findings were addressed in the case narrative and documented in ECM
* Counterparty(ies) were appropriately selected and screened, and all relevant research and findings were addressed in the case narrative and documented in ECM
* The transaction analysis was thoughtfully performed, including identification and documentation of appropriate transaction patterns, account history, and red flags
* The documentation recorded in ECM is accurate and comprehensive, including due diligence on the Focal Entity and Counterparty(ies), dispositioning of OFAC screening results and negative news as applicable, and other supporting documentation, as applicable
* The conclusion reached by the Investigator is appropriate and aptly documented in the alert closure/alert referral form
* All alerts were dispositioned and the rationale(s) for determining whether the alert was suspicious or not suspicious was suitably provided
* The generated Case Narrative was reviewed for accuracy and aligns with investigation findings, wherein the narrative includes all required elements identified by the respective instructions and templates and the Case Disposition aligns with the dispositions in Alert Review (see 5.1.viii)
* The Investigator complied with the Lookback Procedures, and appropriately investigated, dispositioned, and documented their decision on the case

1. Once the QC 2 Analyst has completed their review:
2. QC 2 Analysts will complete the QC 2 Checklist, attesting that all tabs have been reviewed and feedback has been added to the QC sections.
3. QC 2 Analyst will determine if they agree with the Investigator’s case classification based on the transaction analysis, the research conducted, and supporting documentation compiled. The QC 2 Analyst has three options for reviewing an alert:

* Return the case to the Investigator for rework ensuring that feedback is included in the QC feedback boxes in each tab. Select “Returned – Revisions Required” in the ECM workflow to move the case back to the Investigator for rework.
* Accept the Investigator’s recommendation to close the alert as not suspicious. Select “Not Suspicious” in the ECM workflow to close the case and record final disposition.
* Agree with the recommendation for a SAR and initiate a referral to Green Dot for potentially suspicious activity. Select “Decision in Progress” under GD Compliance in the ECM workflow to move the case to Green Dot FIU to review SAR recommendation.

**6. Case Referral to Green Dot and Closing Cases with Potential Suspicious Activity**

**6.1 Escalation to SAR:** In the event that potential suspicious activity is identified, the Case will be referred to Green Dot Senior Management for review and determination of whether a SAR will be filed

1. On a weekly basis (or more frequently, as needed), Lookback Senior Management will present all cases identified in the previous week as suspicious)
2. Green Dot Leadership will review and determine whether a SAR will be filed
3. Upon receiving confirmation of whether a SAR will be filed by Green Dot, Lookback Senior Management (or a delegate) will inform the assigned QC 2 Analyst of the decision
4. The QC 2 Analyst will:
   1. Navigate to ECM, and navigate to each case in the status “GD Compliance – Decision in Progress”
   2. If Green Dot intends to file a SAR, click “SAR Filed”
   3. Move the case the case to “Case Closed – Potentially Suspicious”

**Appendices**

**Appendix A: Transaction Monitoring Rules**

|  |  |  |
| --- | --- | --- |
| Rule ID # | Rule Name | **Description** |
| **1** | **Cash Structuring / CTR Evasion** | Identifies instances of a customer engaging in 2 or more cash deposit transactions (or 2 or more cash withdrawal transactions) in amounts greater than or equal to $1,000 and under $10,000 that aggregate to $10,000 or more during a 7-day rolling period |
| **2** | **Change in behavior** | Identifies instances where the customer transacts at a level three standard deviations above their 15-month average; and, where alerts are only generated if the month is above $10,000 ($5,000 for Supplemental) and the customer triggered in more than 1 month |
| **3** | **Excessive foreign ATM usage** | Identifies instances where a customer withdraws or deposits funds to/from non-U.S. ATMs (including withdrawals and deposits conducted in US territories, such as US Virgin Islands) that aggregate to over $1,900 over a rolling 7-day period |
| **4** | **Multiple Location Deposits and Withdrawals** | Identifies instances of a customer depositing or withdrawing cash (cash, e-cash, checks, ATM withdrawals), at 4 or more retail locations (including merchant stores, checking cash locations, ATMs, or any place where one has access to deposit or withdrawal) aggregating to $1,350 over a 3-day rolling period |
| **5** | **Excessive Foreign POS Usage** | Identifies instances where a customer conducts POS transactions (i.e., all card transaction types where the purchase is a physical POS) outside of the US (including withdrawals conducted in US terrorities, such as US Virgin Islands), that aggregate to over $1,300 over during a 7-day rolling day period |
| **6** | **Layering (One to Many / One to One)** | Identifies instances of a customer receiving / depositing a single amount of $6,000 and then sending that amount across multiple transactions aggregating to between 90% and 110% of that amount within a 7-day period |
| **7** | **Funneling (Many To One / One to One)** | Identifies instances of a customer receiving funds across multiple transactions and then sending the aggregated single transaction within 90% to 110% of that amount within a 7-day period |
| **8** | **Rapid movement of funds** | Identifies customers with transactions within a 14-day period and the total amount of outgoing transactions greater than or equal to 90% of the total amount of the incoming transactions. And where the total of incoming transactions is greater than or equal to $7,000. |
| **9** | **Excessive bill payments - Value** | Identifies instances of a customer making aggregated high value ($5,000) bill payment in a calendar month. |
| **10** | **Exclusive Relationship (P2P)** | Identifies instances of a customer with aggregated at month level activity with a single counterparty constitutes 80% or more of the customer's aggregate P2P transaction amount. Additionally, total dollar value of transactions between the customer and the counterparty are greater than or equal to $7,500. (Excludes self transfers - account to account transfers within same MCID). |
| **11** | **Structured payments to avoid detection (P2P)** | Identifies instances of multiple transactions between a customer and a single counterparty (different MCIDs) within a 7-day rolling period that consists of multiple small dollar amount transactions greater than or equal to $100 and aggregating to a large dollar amount >= $9,000. This activity can be indicative of an attempt to break down large amounts into smaller amount transactions to avoid detection. |
| **12** | **Excessive Internal Transfers (P2P)** | Identifies potentially unusual internal transfers amongst accounts with the same MCID within a 14-day rolling period, aggregating in transaction amount of >= $10,000. |
| **13** | **Roundtrip Payments between the Same Originator and Same Beneficiary (P2P)** | Identifies payments greater than $5,000 that originates from one counterparty to another counterparty and then sent back by that counterparty to the original counterparty 90% to 110% of that amount within a 7-day rolling period. |
| **14** | **High transaction volume** | Identifies high transaction volume customers with 50 or more debits or credits (e.g., ACH, wires, EFTs) within a 7-day rolling period, where the value of each transaction is >=$1,000. |
| **15** | **Change in Behavior Bill Pay** | Identifies instances where the customer transacts in bill pay transactions at a level two standard deviations above their 15-month average; and, where alerts are only generated if the month is above $3,000 and the customer triggered in more than 1 month |
| **16** | **High value EFTs** | Identifies highest transactors -- aggregate value of EFTs within a month exceeds $34,000 |
| **17** | **High value Cash** | Identifies highest cash transactors - aggregate value of cash within a calendar month exceeds $5,000 ($4,000 supplemental) |
| **18** | **High value Checks** | Identifies highest transactors -- aggregate value of checks within a calendar month period exceeds $11,000 |
| **19** | **Change in behavior - Checks** | Identifies instances where the customer transacts in checks at a level two standard deviations above their 15-month average; and, where alerts are only generated if the month is above $2,000 and the customer triggered in more than 1 month. |

**Appendix B: Common Transaction Monitoring Red Flags**

**Funds Transfers**

* Many funds transfers are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
* Activity occurs to/ from/in a higher-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer’s business or history.
* Activity occurs to or from a financial institution located in a higher risk jurisdiction distant from the customer's operations.
* Many small, incoming transfers of funds are received, or deposits are made using checks. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with the customer’s business or history.
* Large, incoming funds transfers are received on behalf of a foreign client, with little or no explicit reason.
* Funds transfer activity is unexplained, repetitive, or shows unusual patterns.
* Payments or receipts with no apparent links to legitimate contracts, goods, or services are received.
* Funds transfers are sent or received from the same person to or from different accounts.
* A customer deposits funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into a master account and transferred outside of the country, particularly to or through a location of specific concern (e.g., countries designated by national authorities and Financial Action Task Force on Money Laundering (FATF) as noncooperative countries and territories).

**Activity Inconsistent with the Customer’s Business**

* The currency transaction patterns of a business show a sudden change inconsistent with normal activities.
* A large volume of transfers is deposited into, or purchased through, an account when the nature of the accountholder’s business would not appear to justify such activity.
* A retail business has dramatically different patterns of transactions from similar businesses in the same general location.
* Unusual transfers of funds occur among related accounts or among accounts that involve the same or related principals.
* Goods or services purchased by the business do not match the customer’s stated line of business.

**Shell Company Activity**

* A bank is unable to obtain sufficient information or information is unavailable to positively identify originators or beneficiaries of accounts or other banking activity (using Internet, commercial database searches, or direct inquiries to a respondent bank).
* Payments to or from the company have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
* Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers.
* Unusually large number and variety of beneficiaries are receiving funds transfers from one company.
* Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk offshore financial centers.
* Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
* Purpose of the shell company is unknown or unclear.

**Other Unusual or Suspicious Customer Activity**

* Customer purchases a number of open-end prepaid cards for large amounts. Purchases of prepaid cards are not commensurate with normal business activities.
* Customer receives large and frequent deposits from online payments systems yet has no apparent online or auction business.
* Suspicious movements of funds occur from one bank to another, and then funds are moved back to the first bank.
* Currency is deposited or withdrawn in amounts just below identification or reporting thresholds.
* Customer repeatedly uses a location (e.g., Walmart, Bank ATM) that is geographically distant from the customer's home or office without sufficient business purpose.
* Customer uses a personal (consumer) account for business purposes.
* Customer has established multiple accounts in various corporate or individual names that lack sufficient business purpose for the account complexities or appear to be an effort to hide the beneficial ownership from the bank.
* Customer makes multiple and frequent deposits to various accounts that are purportedly unrelated.
* Customer conducts large deposits and withdrawals during a short time period after opening and then subsequently closes the account or the account becomes dormant. Conversely, an account with little activity may suddenly experience large deposit and withdrawal activity.
* Customer makes high-value transactions not commensurate with the customer's known incomes.

**Potentially Suspicious Activity That May Indicate Terrorist Financing**

**Activity Inconsistent With the Customer’s Business**

* Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
* The stated occupation of the customer is not commensurate with the type or level of activity.
* Persons involved in transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
* Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

**Funds Transfers**

* A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
* Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
* Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

**Other Transactions That Appear Unusual or Suspicious**

* Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
* Funds are sent or received via international transfers from or to higher-risk locations.

**Appendix C: Common Definitions**

* **Suspicious Activity Report (“SAR”):** A report filed by financial institutions to regulators when suspicious or potentially suspicious activity is detected.
* **Know Your Customer (“KYC”):** The process of verifying the identity of clients and assessing potential risks of illegal intentions in the business relationship.
* **Customer Due Diligence (“CDD”):** Procedures used to collect and evaluate relevant information about a customer to assess their risk profile.
* **Customer Identification Program (“CIP”):**
* **Currency Transaction Report (“CTR”):** A report that U.S. financial institutions must file for each transaction in currency of more than $10,000.
* **Office of Foreign Assets Control (“OFAC”):** A U.S. Treasury office that administers and enforces economic and trade sanctions.
* **Financial Intelligence Unit (“FIU”):** A government agency responsible for receiving, analyzing, and disseminating financial information to combat money laundering and terrorist financing.
* **Bank Secrecy Act(“BSA”):** U.S. legislation that requires financial institutions to assist government agencies in detecting and preventing money laundering.
* **PATRIOT Act:** U.S. law that, among other things, strengthens AML requirements for financial institutions.
* **Politically Exposed Person (“PEP”):** An individual who holds a prominent public position and may present a higher risk for potential involvement in bribery or corruption.
* **Alert:** A notification generated by a TMS indicating a transaction or pattern that may require further investigation.
* **C2C (Consumer-to-Consumer):** refers to transactions where consumers buy and sell goods or services directly from each other, often through online platforms like eBay or Craigslist. These transactions bypass traditional retailers and allow consumers to directly connect with each other for sales.
* **Case Management:** The process of tracking, investigating, and resolving alerts or cases generated by transaction monitoring.
* **False Positive:** An alert or case flagged as suspicious by the system but determined to be legitimate after investigation.
* **Typology:** A pattern or method commonly used in money laundering or financial crime.

**Appendix D: High Risk Countries**

|  |  |  |
| --- | --- | --- |
| **High-Risk Jurisdictions** |  |  |
| **Country** | **Rationale** | | **2nd Rationale** |
| **Afghanistan** | **Sanctions** | |  |
| **Algeria** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Angola** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Balkans** | **Sanctions** | |  |
| **Belarus** | **Sanctions** | |  |
| **Benin** | **Sanctions** | |  |
| **Bosnia and Herzegovina** | **Sanctions** | |  |
| **Botswana** | **Sanctions- Check against UK list** | |  |
| **Bulgaria** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Burkina Faso** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Burma (Myanmar)** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Cameroon** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Cape Verde** | **Sanctions- Check against UK list** | |  |
| **Central African Republic** | **Sanctions** | |  |
| **China** | **Sanctions** | |  |
| **Congo** | **Sanctions** | |  |
| **Cote D’Ivoire** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Croatia** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Democratic Republic of the Congo** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Cuba** | **Sanctions** | |  |
| **Equatorial Guinea** | **Sanctions** | |  |
| **Ethiopia** | **Sanctions** | |  |
| **Haiti** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Hong Kong** | **Sanctions** | |  |
| **Iran** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Iraq** | **Sanctions** | |  |
| **Kenya** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Lao People's Democratic Republic** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Lebanon** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Libyan Arab Jamahiriya** | **Sanctions** | |  |
| **Macedonia** | **Sanctions** | |  |
| **Montenegro** | **Sanctions** | |  |
| **Mali** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Monaco** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Mozambique** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Namibia** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Nepal** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Nicaragua** | **Sanctions** | |  |
| **Nigeria** | **Higher Risk AML FATF Black/Grey List** | |  |
| **North Korea** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Palestine** | **Sanctions** | |  |
| **Russian Federation** | **Sanctions** | |  |
| **Serbia** | **Sanctions** | |  |
| **Somalia** | **Sanctions** | |  |
| **South Africa** | **Higher Risk AML FATF Black/Grey List** | |  |
| **South Sudan** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Sudan** | **Sanctions** | |  |
| **Syria** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Tanzania, United Republic of** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Ukraine** | **Sanctions** | |  |
| **Venezuela** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Vietnam** | **Higher Risk AML FATF Black/Grey List** | |  |
| **Yemen** | **Higher Risk AML FATF Black/Grey List** | | **Sanctions** |
| **Yugoslavia** | **Sanctions** | |  |
| **Zimbabwe** | **Sanctions** | |  |

**Appendix E: Case Narratives**

**GD Closure Narrative**

**Introduction**

**Case:** 123456

**Summary**

Case 123456 violated X number of rules, has X number of alerts, and the alerting transactions totaled $X. Review determined the activity is not suspicious and the case is being recommended for closure. Alerts 1, 2, and 3 (collectively, the “Alerts”) alerted for Rule 1 and Rule 2. The alerted activity consisted of XX transactions between XX/XX/XXXX and XX/XX/XXXX, totaling $XX,XXX.

*Insert table with the rules and alerts*

The Cases do not appear to be suspicious because research indicates that [insert rationale, e.g., Focal Entity A works in the electronics industry and the three counterparties sell electronic components].

**Rule Summary:**

Rule 1 is designed to identify [insert rule description] while Rule 2 is designed to identify [rule description]. However, the activity does not appear suspicious because:

* Rule 1: [closure rationale: e.g., research identified the focal entity and counterparties, the focal entity and counterparties operate in complementary lines of business of {insert business types}, and the activity had an apparent economic purpose].
* Rule 2: [closure rationale: e.g., research identified the focal entity and counterparties, the focal entity and counterparties operate in complementary lines of business of {insert business types}, and the activity had an apparent economic purpose].

**Focal Entity Summary:**

Research indicated that Focal Entity A is located in [Location], and is in engaged in the [Industry] business. Between [Date] and [Date], Focal Entity A conducted X transactions totaling $Y to Z counterparties located in [Region]. Negative news was conducted using LexisNexis and Google. No adverse media was identified for Focal Entity A.

**Sampled Counterparty Summary:**

Counterparties 1, 2, 3, 4, 5, 6 were chosen for sampling because they are the [insert rationale, e.g., highest value/volume counterparties]. No adverse media was identified for the Counterparties.

**Counterparty 1:**

Research indicated that Counterparty 1 is located in [Location], and is in engaged in the [Industry] business. Between [Date] and [Date], Focal Entity A conducted X transactions with Counterparty 1 totaling $Y. Negative news was conducted using LexisNexis and Google.  No adverse news was identified for Counterparty 1.

*[Repeat for each Counterparty]*

**Conclusion**

Based on the above research, the alerts are recommended for closure as the activity does not appear suspicious, given the following: [Insert rationale at a high level – counterparty demographic, patterns of activity, etc.]

**GD Escalation Narrative**

**Introduction**

**Case:** 123456

**Summary**

Case 123456 violated X number of rules, has X number of alerts, and the alerting transactions totaled $X. Review determined the activity is potentially suspicious and the case is recommended for SAR filing. Alerts 1, 2, and 3 (collectively, the “Alerts”) alerted for Rule 1 [rule name] and Rule 2 [rule name]. The alerted activity consisted of XX transactions between XX/XX/XXXX and XX/XX/XXXX, totaling $XX,XXX.

*Insert table with the rules and alerts*

The alerts appear potentially suspicious because [insert rationale, e.g., the transaction activity includes an unusual pattern of incoming or outgoing transaction activity] and because [insert rationale 2, e.g., research identified adverse news associated with Counterparty 1].

**Rule Summary:**

This case alerted for Rule 1, which is designed to identify [insert rule description], and Rule 2, which is designed to identify [insert rule description].

The following indicators of potentially suspicious activity were observed:

* Rule 1: [escalation rationale: e.g., research could not identify the focal entity and counterparties, the focal entity and counterparties could not be connected, and found no economic purpose for the activity].
* Rule 2: [escalation rationale: e.g., research could not identify the focal entity and counterparties, the focal entity and counterparties could not be connected, and found no economic purpose for the activity].

**Focal Entity A:**   
Research indicated that Focal Entity A is located in [Location] and is engaged in the [Industry] business. Between [Date] and [Date], Focal Entity A conducted X transactions totaling $Y to Z counterparties located in [Region]. Negative news was conducted using LexisNexis and Google. [Adverse media was identified for Focal Entity A; no adverse media was identified for Focal Entity A]. [Summary of Adverse Media].

**Sampled Counterparty Summary:**

Counterparties 1, 2, 3, 4, 5, 6 were chosen for sampling because they are the [insert rationale, e.g., highest value/volume counterparties]. No adverse media was identified for the Counterparties.

**Counterparty 1:**

Research indicated that Counterparty 1 is located in [Location] and is engaged in the [Industry] business. Between [Date] and [Date], Focal Entity A conducted X transactions with Counterparty 1 totaling $Y. Negative news was conducted using LexisNexis and Google. [Adverse media was identified for Counterparty 1; no adverse media was identified for Counterparty 1]. [Summary of Adverse Media].

[Repeat for each Counterparty]

**Conclusion**

Based on the above research, the case is recommended for SAR filing as the activity appears potentially suspicious, given the following: [Insert rationale at a high level – counterparty demographic, patterns of activity, etc.]

XX transactions between XX/XX/XXXX and XX/XX/XXXX are being recommended for escalation.

Attach File:

[Insert table with escalated transactions and attach to ECM as a csv ]– Refined transaction file that only includes transactions associated with potentially suspicious alerts.]

Appendix F: Change Log

6/17/2025 (WA + AG)

* Updated 4.2.9 language to “Escalation Recommended” instead of “Suspicious”
* Modified section related to the Bot and recommended comments.
* Added Change Log Appendix section.
* Updated 4.2.6 language to mention the Z Drive.
* Added footnote to 4.2.4 e that references String Search Bot instructions from Gopal. (sent the email on 6/17/25)

6/19/2025 WA

* Naming Conventions formatting has been updated throughout the document to reflect “MM.DD.YYYY”
* 6/20/2025 WA
* In 4.2.2, comment added about well known entities not being valid for the counterparty selection, included the list in the footnote.
* Updated document to reflect new naming convention: Document Description \_ Party/Focal Entity/Counterparty/ Date MM-DD-YYYY

6/24/2025

* New version of the procedures 1.3
* New guidance related to Bot search started on 6/24/2025, to include State in search.

6/26/2025

* Updated section on searches to add that the focal entities and counterparties should be in quotes. (e.g. “John Smith”)

1. Well-known merchants include: Walgreens, CVS Pharmacy, Rite Aid, Dollar General, Family Dollar, Kroger (and affiliates: Fry’s, King Soopers, Ralphs, Smith’s, etc.), Safeway (and affiliates: Vons, Albertsons, Randalls, Tom Thumb, etc.), 7-Eleven, Speedway, Circle K, Kwik Trip/ Kwik Star [↑](#footnote-ref-2)
2. Focal entity is defined as the Focal Entity(ies) listed as the primary account holder/signer, the secondary account holder/signer, and, for SMB products, the affiliated entity. [↑](#footnote-ref-3)
3. An account may be closed at time of review but was open at the time of the Lookback. [↑](#footnote-ref-4)
4. As noted above, CIP information may vary by account. Consideration should be taken of this cross-count variation, especially any discrepancies that may indicate potential suspicious account opening or indicative of potential fraud (e.g., multiple e-mails, different DOB). [↑](#footnote-ref-5)
5. In ECM, to download, you may be prompted to enter your sign in information. You should use your DC1 account: dc1[username]@dc1.greendotcorp.com [↑](#footnote-ref-6)
6. While a certain type of activity may have alerted (e.g., cash withdrawals), the Focal Entity(ies) may have a history of conducting similar activity that did not alert. Use the Lookback Transaction Summary to help identify months that may have similar activity and download non-alerting transactions using “Download Historic Transaction Table” [↑](#footnote-ref-7)
7. An alert is a ***false positive*** if the alert transactions do not meet the criteria for the scenario or alert erroneously [↑](#footnote-ref-8)
8. Since not all Green Dot transactions contain time stamps, transactions occurring on the same day should be considered simultaneous. [↑](#footnote-ref-9)
9. If additional transactions navigate to the Statistic Page and download the 15-month transaction history from “Download Historic Transaction Table” under Lookback Period Data. [↑](#footnote-ref-10)
10. In some cases, there may not be a valid counterparty to select, including when the only transacting parties are well-known entities (e.g., Walmart) or the transacting party data indicates an activity descriptor. [↑](#footnote-ref-11)
11. Well-Known Entities are defined under the definition of “customer” for Banks found in 31 CFR 1020.100 – Definitions for the Customer Identification Program, and include the following:

    A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator;

    A department or agency of the United States, of any State, or of any political subdivision of any State; any entity established under the laws of the United States, of any State, or of any political subdivision of any State, or under an interstate compact between two or more States, that exercises governmental authority on behalf of the United States or any such State or political subdivision; and

    Any entity or wholly owned subsidiary, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stock or interests listed under the separate “NASDAQ Capital Markets Companies” heading), provided that a person that is a financial institution, other than a bank, is exempt only to the extent of its domestic operations.

    Additionally, based on their role as merchants for processing Green Dot cash back transactions, the following entities will also be considered a Well Known entity: Walmart, Walgreens, CVS Pharmacy (CVS), Rite Aid, 7-Eleven, Dollar General, Family Dollar, Kroger (and affiliates: Fry’s, King Soopers, Ralphs, Smith’s, etc.), Safeway (and affiliates: Vons, Albertsons, Randalls, Tom Thumb, etc.), Speedway, Circle K, Kwik Trip / Kwik Star [↑](#footnote-ref-12)
12. Counterparty address can be determined based on [↑](#footnote-ref-13)
13. In order to get the macro to function, following the instructions below.

    Save the file in your my documents folder

    Open Chrome and enter cntrl + P (the print shortcut) and ensure that the Destination is selected as ‘Microsoft Print to PDF’. Once this is selected click ‘Print’ and save the file to a folder where you would want the PDF files to be saved.

    Right click on the excel macro file and select ‘Properties’. In the properties window, click the ‘Unblock’ checkbox and click ‘apply and ‘ok’.

    Open the Macro and enter the names of the entities/ individuals that you want to screen and click Run. Please wait for the ‘Done’ notification from the macro before interacting further with your system.

    The screening PDF’s should be available in the folder that was manually selected in step 2. [↑](#footnote-ref-14)
14. The string search is considered as follows: “Name of the Individual/Entity” AND “Investigations” OR “Bribery” OR “Fraud” OR “Laundering” OR “Criminal” OR “Terrorist” OR “Evasion” OR “Indictment” OR “Regulatory” OR “Court” OR “Court Case” OR “Arrest” OR “Litigation” OR “Murder” OR “Defendant” OR “Felony” OR “Bankruptcy” OR “Crime” OR “Compliant

    ” [↑](#footnote-ref-15)
15. For purposes of the Lookback, the following types of adverse news are considered non-relevant:

    Civil litigations or fines for violations that are not related to financial crimes.

    Assault, domestic violence, misdemeanors, or other crimes that are not related to the transaction activity. [↑](#footnote-ref-16)
16. For purposes of the Lookback, the following types of adverse news are considered relevant:

    Money laundering or terrorist financing

    Corruption or bribery

    Association with terrorist groups

    Regulatory fines and actions

    Embezzlement or misappropriation of funds

    Fraudulent activity or other financial crimes

    Sanctions circumvention

    Drug/human/arms/blood diamond/other trafficking

    * Activity typically comprising a felony

    [↑](#footnote-ref-17)
17. For purposes of the Lookback, the following types of adverse news are considered non-relevant:

    Civil litigations or fines for violations that are not related to financial crimes.

    Assault, domestic violence, misdemeanors, or other crimes that are not related to the transaction activity. [↑](#footnote-ref-18)
18. For purposes of the Lookback, the following types of adverse news are considered relevant:

    Money laundering or terrorist financing

    Corruption or bribery

    Association with terrorist groups

    Regulatory fines and actions

    Embezzlement or misappropriation of funds

    Fraudulent activity or other financial crimes

    Sanctions circumvention

    Drug/human/arms/blood diamond/other trafficking

    * Activity typically comprising a felony

    [↑](#footnote-ref-19)
19. Note, if no results are present, the PDF should be saved [↑](#footnote-ref-20)