Sass Society Inc d/b/a Wishes

Transaction Monitoring Procedures

Effective May 2024

Version 1.0

Contents

1. Company Description

Sass Society Inc d/b/a Wishes ("Wishes" or the "Company") was established to offer a platform to allow an individual, or nonprofit organization (the "Organizer") to post a fundraiser ("Fundraiser") to the Platform to accept monetary donations ("Donations") from donors ("Donors") on behalf of the beneficiaries of the Fundraiser ("Wishers"). The Company facilitates the Fundraiser of the Organizers and permits Donors to make donations to these Fundraisers.

2. Overview

This document describes the Company's Transaction Monitoring ("TM") process. These procedures are designed to implement Wishes' policies covering Bank Secrecy Act ("BSA"), Anti-Money Laundering ("AML"), and Office of Foreign Assets Control Compliance ("OFAC") as it relates to monitoring illicit activity on Wishes' platform.

3. Purpose

The purpose of this document is to establish and manage Wishes' transaction monitoring process in accordance with the Company's BSA/AML/OFAC Policy ("AML Policy"). Additionally, this process document will cover the necessary actions and reporting required by Wishes' bank partner(s).

Transaction monitoring allows Wishes to monitor users and customer profiles and their transactions on a regular basis for AML and OFAC risks. By combining this information with analysis of customer historical data and Organizer account profiles, it can provide Wishes with a holistic view of Organizers' profiles, risk levels, and predicted future activity, and can also generate information for reporting and create alerts to detect potentially suspicious activity.

The transactions monitored include card payments and other transactions occurring on Wishes' platform. Transaction monitoring also includes watch list screening ("sanctions screening"), internal watch list ("Watchlist"), and customer profiling.

When specifically used, the term "customer" refers to both Organizers and Donors within this Policy.

4. Roles

Compliance Analyst: reviews the Organizer's transaction activity, unusual activity, conducts alert review, investigation, and handles documentation and escalation of unusual activity to the Chief Compliance Officer.

Chief Compliance Officer ("CCO"): reviews the escalations made by the Analysts and has the authority to appoint a designee, review the escalations made by the Analysts, make case-by-case determinations, and report information to appropriate internal and external parties, bank partners, and appropriate law enforcement agencies.

In the event that the designated CCO is unavailable or unable to authorize approvals or perform tasks typically conducted by the CCO or as noted within this Procedure or the AML Policy, Wishes' Founder will have the authority to act as the designated CCO in a temporary capacity.

Compliance Department ("Compliance"): The Compliance Department is responsible for documenting the unusual activity detected and its disposition as outlined in this Procedure. The Compliance Department for Wishes is made up of the CCO and Ankura Consulting's Federal Compliance Team (Third-party support as needed), acting as Analysts.

5. Responsibilities

Wishes' CCO is the designated individual for the AML Program and is responsible for the day-to-day management and operations of the Compliance function and the oversight of the AML Program. The CCO may designate individuals within the Compliance Department to perform certain functions and tasks to execute the program requirements.

The Compliance Department is responsible for administrating the AML Program within the appropriate time frames under the direction of the CCO and seeking approvals as necessary.

6. Transaction Monitoring Overview

Wishes monitors for money laundering, terrorist financing, and other illegal activity associated with customers and their transactions on an ongoing basis, using a monitoring system and human review.

The automated TM system used by the Company is SardineAI Corp (customarily known as "Sardine") and is coded to run rules and employs machine techniques to detect irregular activity. Sardine is programmed by Wishes to identify transactions which appear to be:

- Unusually high dollar amounts;
- Part of an unusual pattern of transactions;
- Potential fraud; and
- Appear to have no apparent economic or visible lawful purpose.

Another element of the Company's internal control is watch list and database monitoring. The Company screens its database of Organizers and Donors to:

- Identify prohibited Organizer types;
- Identify Organizers with higher risk characteristics; and/or,
- Establish/confirm expectations for customer behaviors.

Records and reports used in the monitoring of Donor activity are notated to evidence review. These notations will indicate:

- Whether the activity appears to be normal for the Organizer's Fundraiser;
- Whether the activity can be explained for or by the Organizer; and/or
- Whether additional monitoring and/or research are warranted.

6.1. Monitoring Frequency

Transactions occurring on the platform will be screened by the TM system in real time and reviewed by Wishes' Analysts on a regular, ongoing basis. Additional reviews of historical data will also be conducted by the CCO on a periodic basis for in-depth identification of trends and patterns to inform specific risk mitigation techniques tailored to Wishes' business model.

6.2. Review Process

This section provides process guidance in conducting transaction monitoring within Wishes' TM system. The transaction monitoring process contains the following steps:

1. **Triage the Alert** - The Analyst will log into the TM system and review alert information within Sardine.

   The Analyst will review the alert information with the receiver and sender data and include the following information in the review:

   - Executed Rules
   - Total flagged amount
   - Total flagged count
   - Transaction Description
   - Transaction Type

2. **Review Customer Identification Program ("CIP") Information** - As part of the review, the Analyst will assess the Customer Due Diligence ("CDD") information for the Organizers and look for patterns that may indicate AML red flags or fraud; Organizers requiring additional due diligence or Enhanced Due Diligence ("EDD") reviews and to test for potential gaps in controls.

   EDD may also be executed where a discrepancy is observed on CIP, when transaction monitoring identifies an anomaly, on receipt of a subpoena or any other outside inquiry regarding an Organizer or Donor, or in any case where an employee or compliance team member determine that further diligence is warranted based on the circumstances.

   A basic EDD measure the Company may employ, for example, is requesting that the Organizer provide proof of address and purpose of their donor activity; or any other document deemed acceptable by the CCO that allows the Company to form a reasonable belief that it knows the identity of the Organizer and that their accompanying information is true and accurate, and that the activity being initiated is legitimate and not associated with financial crime.

3. **Conduct Transaction Analysis** - Transaction data is analyzed to identify trends and patterns in locations, Organizer and Donor information (when available), and fluctuations in volumes as well as to review for unusual activity.

The Analyst will conduct a review of the Organizer's activity which should include the triggering activity and any historical transactional activity. The activity should be compared to the Organizer's profile information to determine if the activity is normal and expected for that type of Fundraiser.

4. **Escalations** - The Analyst may flag high-risk or unusual activity for further review by the CCO (or designee). Organizers or Donors recommended for ongoing monitoring will be added to the Watchlist by the CCO.

5. **Documentation -** Upon completion of the review, the Analyst will provide a resolution for the alert (see Appendix A for full walkthrough). The Analyst will complete a narrative summary, documenting a summary of their findings/results, and recommendation for disposition of the alert.

6. **Conclusion** – The completed alert will be actioned accordingly, which can include an Analyst closing out the alert, escalating the alert to the CCO for further review, adding a customer to the Watchlist, and/or submitting a referral to its bank partner(s).

The Analyst will document their research/findings and save all supporting documentation within the Sardine platform in accordance with Wishes' retention policy.

Please refer to Appendix A for step-by-step guidance within Sardine[1].

6.3. Enhanced Due Diligence

When Organizers have exceeded a baseline risk level, or are identified as having high-risk or unusual activity, additional due diligence and if applicable, EDD will be completed. The EDD review will include gathering the Organizer's Know Your Customer ("KYC") data, performing searches through internet research or other available sources or tools that would resolve and/or provide a reasonable explanation of the flagged activity.

EDD on the Organizer is performed by conducting one or more of the following activities:

- Internet research using common, reputable search engines (for example Google);
- Searches using other available subscription-based sources or tools;
- Review of additional KYC details not available via the TM system.

Please reference Wishes' AML Policy document for more details regarding the KYC process.

6.4. Reporting

The Compliance Department will provide a summary report of findings for Wishes' CCO or designee to review to ensure that alerts have been dispositioned properly.

[1] Step-by-step guidance was retrieved from Sardine's platform.

Wishes will report on customer and transaction activity to its payment partner(s) as requested.

7. Unusual Activity Overview

Unusual activity reporting is part of the Company's compliance monitoring and reporting responsibilities. Unusual transactions are financial transactions that Wishes has reasonable grounds to suspect are related to conducting money laundering, terrorist financing, or other illegal activity, including fraud.

The Company monitors transactional activity to identify patterns of unusual size, volume, pattern or type of transactions, and geographic factors. The CCO or designee will be responsible for this monitoring, will document when and how it is carried out, and will report potentially unusual activities to the Company's bank partners. The Company provides employee guidelines with examples of money laundering activity and red flags, that may warrant further scrutiny.[2] The CCO or designee will conduct an appropriate investigation before a referral is made to its bank partners.

7.1. Red Flags

The Compliance Department will review the Organizer and their transaction activity to look for red flags deemed unusual that may be indicative of money laundering, terrorist financing, fraud, and other financial crimes. Red flags include but are not limited to those listed below, in addition to guidance from the Financial Crimes Enforcement Network ("FinCEN") and the Federal Financial Institutions Examination Council ("FFIEC") on red flags to look for when reviewing customer and transaction data.

- Activity involves funds derived from illegal activities or is intended or conducted to hide or disguise funds or assets derived from illegal activities;
- Activity is designed to evade the requirements of the Bank Secrecy Act, whether through structuring or other means;
- Activity serves no business or apparent lawful purpose, and the reporting business knows of no reasonable explanation for the transaction after examining all available facts; and/or
- Transactions involve the use of the Company to facilitate criminal activity;
- When any person may be in harm's way.

7.2. Unusual Activity Reporting Responsibilities

The Analyst will notify the CCO promptly when unusual activity is identified. The CCO is also responsible for documenting the unusual activity detected and its disposition as outlined in this document.

The CCO or designee will have the authority to report information to appropriate parties, including to an appropriate law enforcement agency if applicable.

The Company will endeavor to refer unusual activity to its bank partner(s) in accordance with its contractual commitments. Wishes will follow instructions provided by its bank partner(s) regarding their required timing and details and will cooperate in any follow-up investigation to support their filing requirements as applicable.

[2] Please reference Wishes BSA AML OFAC Program Policy for more details.

The Company will maintain a log of referrals to its bank partner(s), including those investigations that may initially have been of concern though were later resolved to have a legitimate explanation or not be suspicious after the collection of all facts.

7.3. Unusual Activity Reporting Process

The CCO or designee will be alerted to unusual activity identified and consider known, relevant details to create a comprehensive view of the activity being reported.

The CCO will work with the Compliance Department to determine when unusual activity warrants a referral to its payment partner(s).

Details to consider when reviewing unusual activity will include the following information:

- How the information was identified
- Date the unusual activity occurred
- Where the unusual activity took place
- The dollar amounts, dates, frequency, volume, counterparties, and jurisdictions involved in the unusual activity
- Any loss amounts, if applicable
- Why the employee deems the activity as unusual
- Organizer profile information (to the extent available) includes the following details:
    - Full name of the Organizer
    - Ultimate Beneficial Ownership (as applicable)
    - Date of birth
    - Address (as applicable)
    - Government identification information (as applicable)
    - SSN/TIN/EIN (as applicable)
    - Email address
    - Any relevant supporting documentation for consideration

The CCO will review the information, along with supporting documentation, and store it for record retention purposes in accordance with Wishes' AML Policy.

7.3.1. Decision Flows

An investigation will be conducted, and the following will occur:

- If the investigation finds that the activity is not unusual, the findings and rationale will be documented and saved as part of the alert file in the Sardine platform.
- If the investigation finds that the activity is not unusual, however requires further review, the Organizer and/or Donor will be placed on the Watchlist for ongoing monitoring by either the Analyst or the CCO.
- If the investigation finds that the activity is potentially suspicious, the Analyst will complete an Incident Report ("IR") form and submit it to the CCO for review. If the IR form is approved by the CCO, this document will serve as the referral form to the Company's bank partner(s). In addition,

the narrative utilized in the IR form may be utilized by the bank partner(s) to file a Suspicious Activity Report ("SAR").

- If the activity is deemed to warrant the closure of the Organizer's account, the Compliance Department will recommend the closure to the CCO or designee. If agreed, the CCO will instruct the prompt closure of account and flag the Organizer profile as a customer restricted from the platform.
- If the account closure is not warranted or recommended at that time, the Organizer (and related Donors, if necessary) will be placed on the Watchlist and monitored for any continuous unusual activity. If unusual activity continues, the Compliance Department will complete a subsequent IR form and refer the customer to their bank partner(s). The CCO will determine the next action(s) for the customer, which can include restriction or closure of the affected account.

Please reference Appendix B for the Incident Report form.

7.3.2. Ongoing Monitoring

If the unusual activity does not result in closing an account, however, warrants further review, the Compliance Department will place the customer on Wishes' Customer Watchlist for ongoing monitoring to determine if the unusual activity continues, with a minimum review period of 90 days.

The Watchlist is Wishes' internal customer watch list that is maintained on Organizers and Donors, identified as requiring ongoing monitoring. Ongoing maintenance and updating of the Watchlist will be the responsibility of the Compliance Department.

Organizers or Donors will be removed from the Watchlist when a resolution is provided and with the approval of the CCO.

Please reference Appendix C for Watchlist.

8. Record Retention

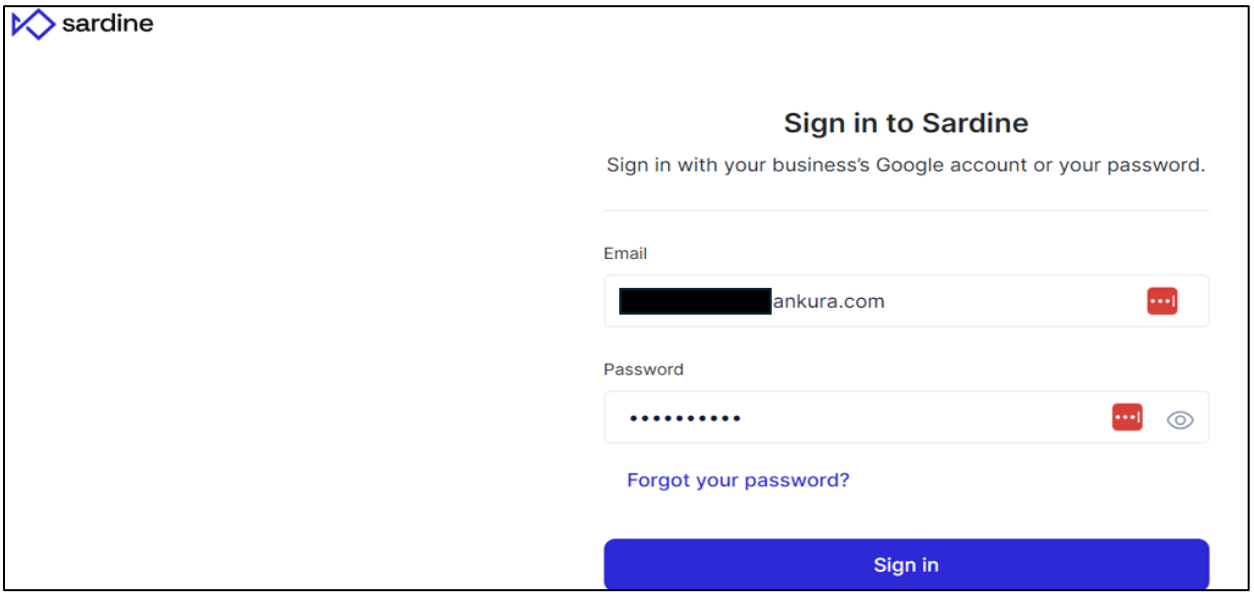
BSA, OFAC, and state regulations require that records and supporting documents be retained for potential review by regulatory agencies for a period of at least five (5) years, unless otherwise noted. This information must be maintained in a manner that permits it to be accessible within a reasonable period of time. It is the Company's policy to retain all required Program documentation including reporting, record keeping, and transaction records for at least five (5) years.

The CCO is responsible for ensuring that all applicable records are maintained securely.

9. Appendix A

9.1. Accessing Sardine

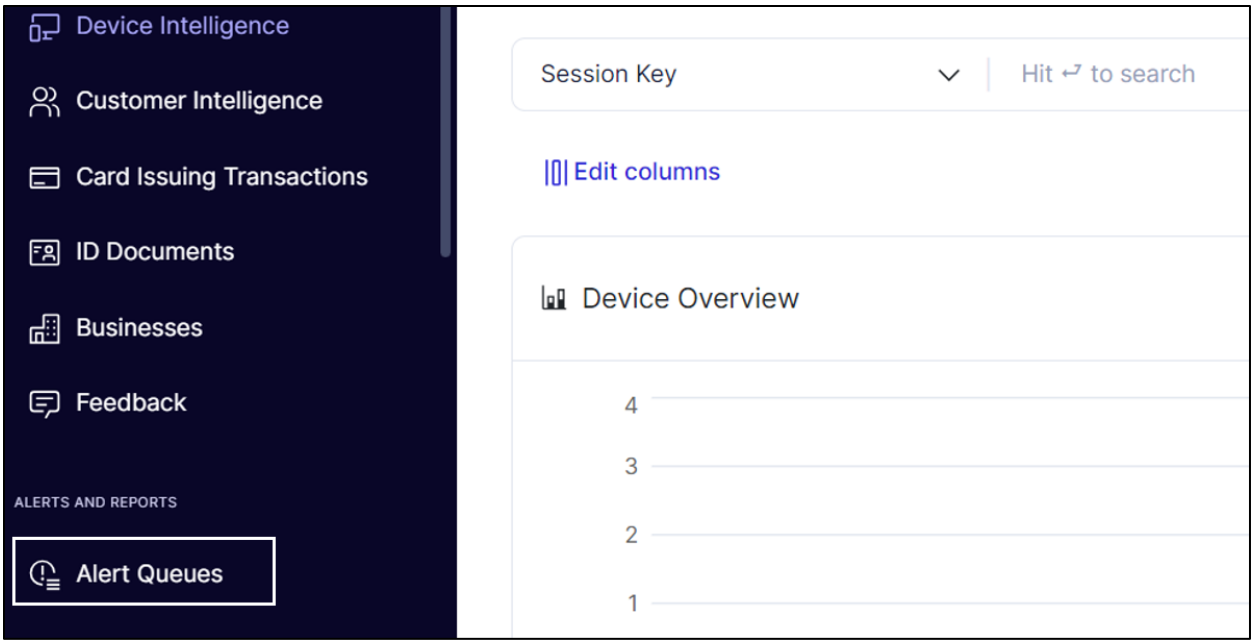
The Analyst will log into Sardine.



9.1.1. Alerts

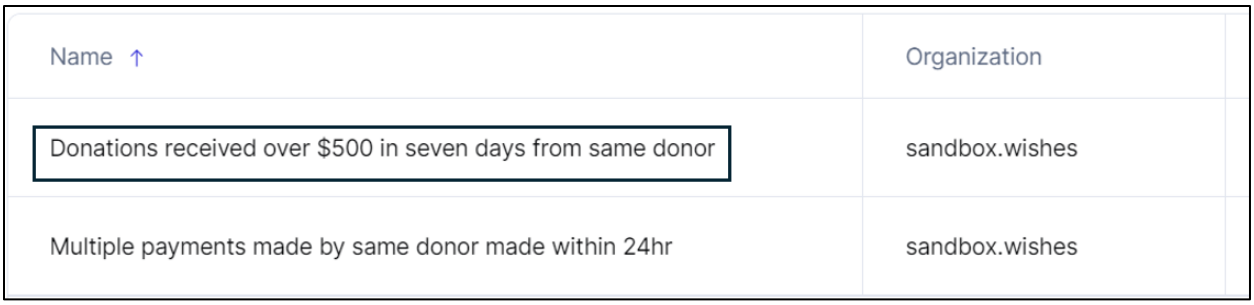
Once logged into Sardine, the Analyst will select “Alert Queues” on the left side of the dashboard.

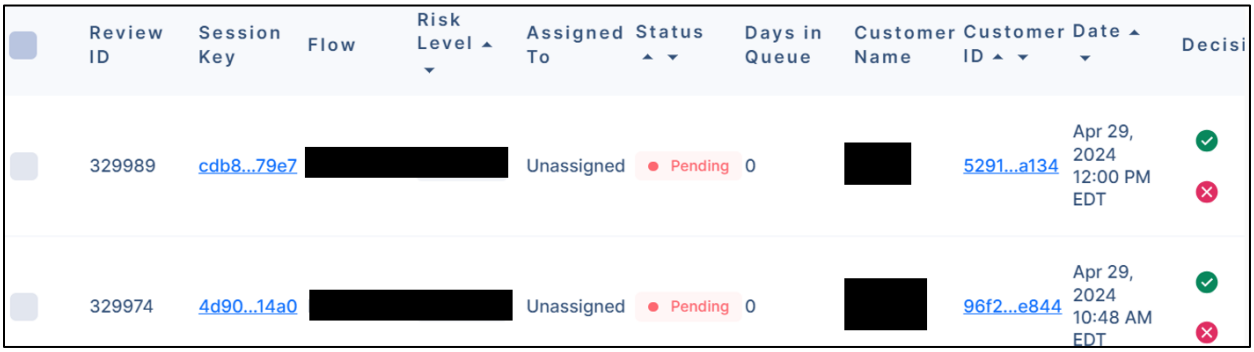
The Alerts Queues page is the first step in the Analyst’s workflow process.



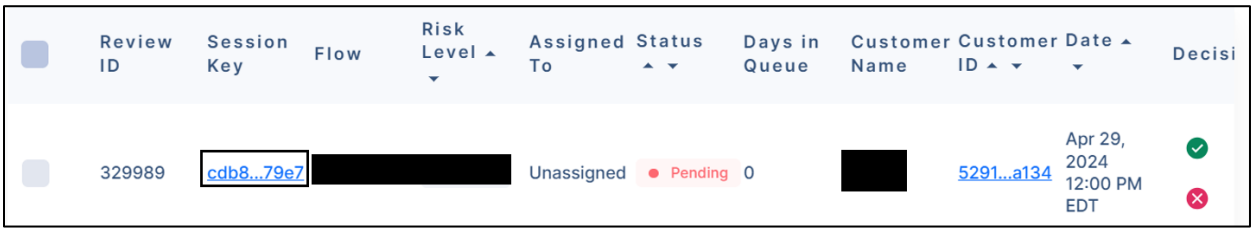
Once the Alerts Queues page is open, scroll to the right to see which queues have unresolved alerts (also called cases in Sardine).

Click on the queue you are reviewing, and the queue will open to show the sessions for each customer with unresolved alerts.

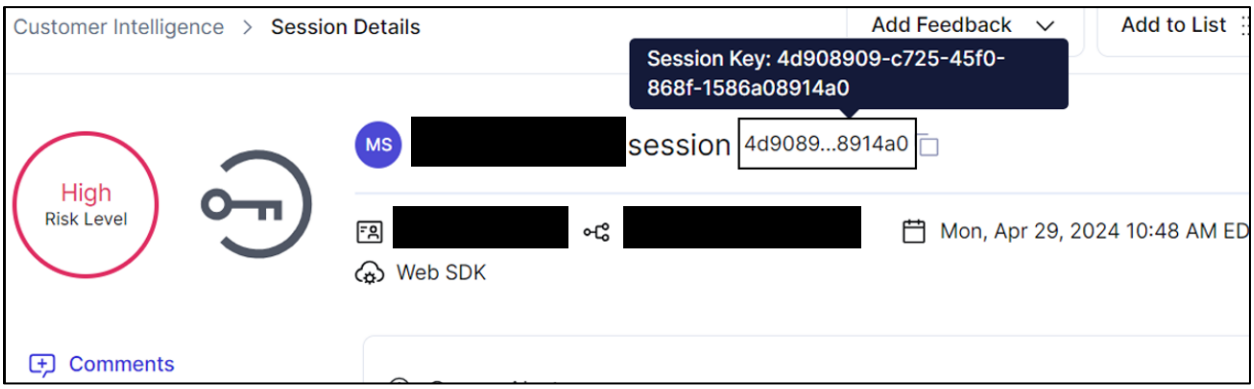




To begin reviewing the session, click on the Session Key link.



Each session is identifiable by a Session Key ID number. Scroll over the information to see the whole number string, if necessary.



When a session is investigated, the Analyst can also find data about:

- The underlying rule(s) and the transactions that triggered the session
- Previously resolved alerts (if needed for additional context)

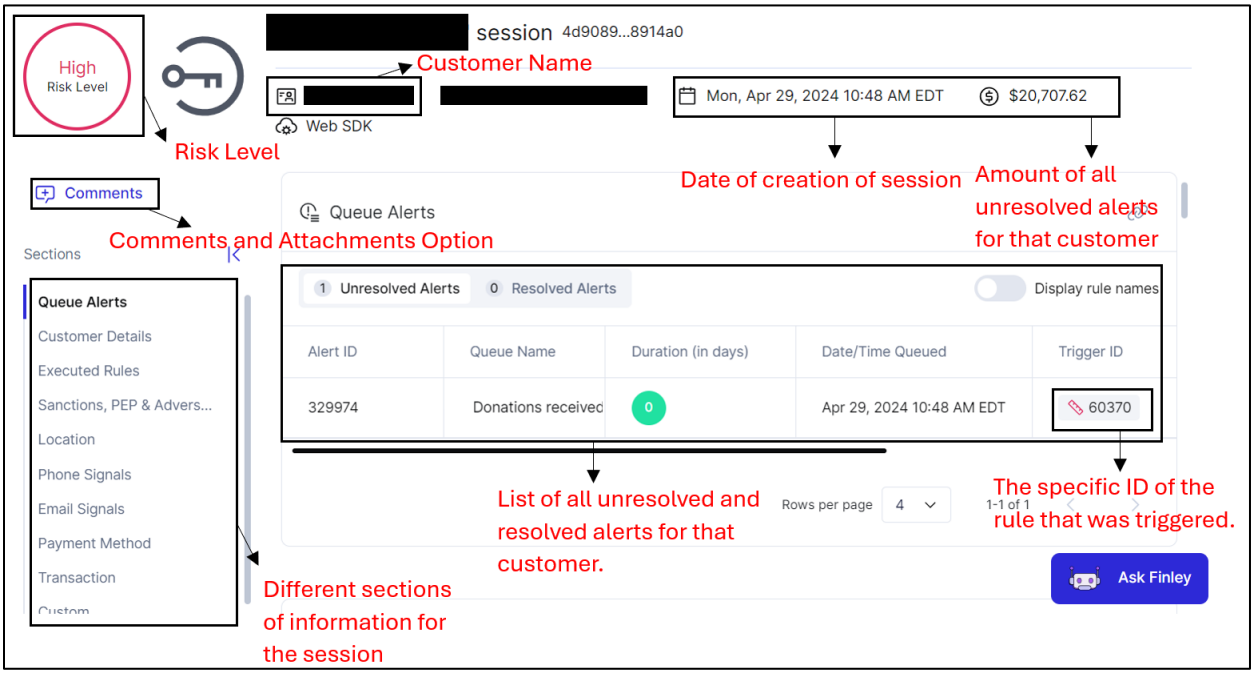
Wishes Transaction Monitoring Procedures

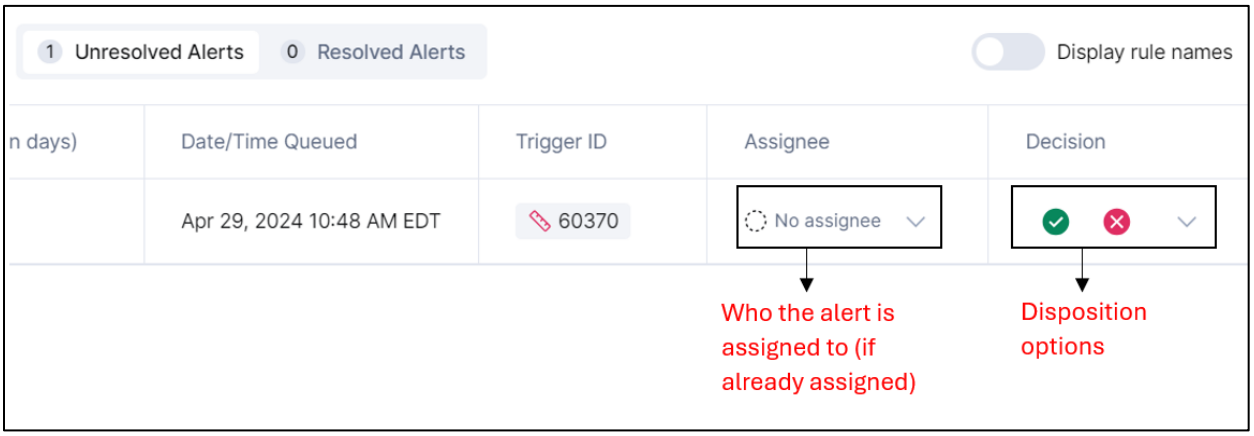
- Entities and instruments involved

During the investigation, the Analyst can:

- Add documents to the alert
- Add notes to the alert
- Re-assign or re-queue the alert
- Resolve the alert

9.2. Overview of a Session

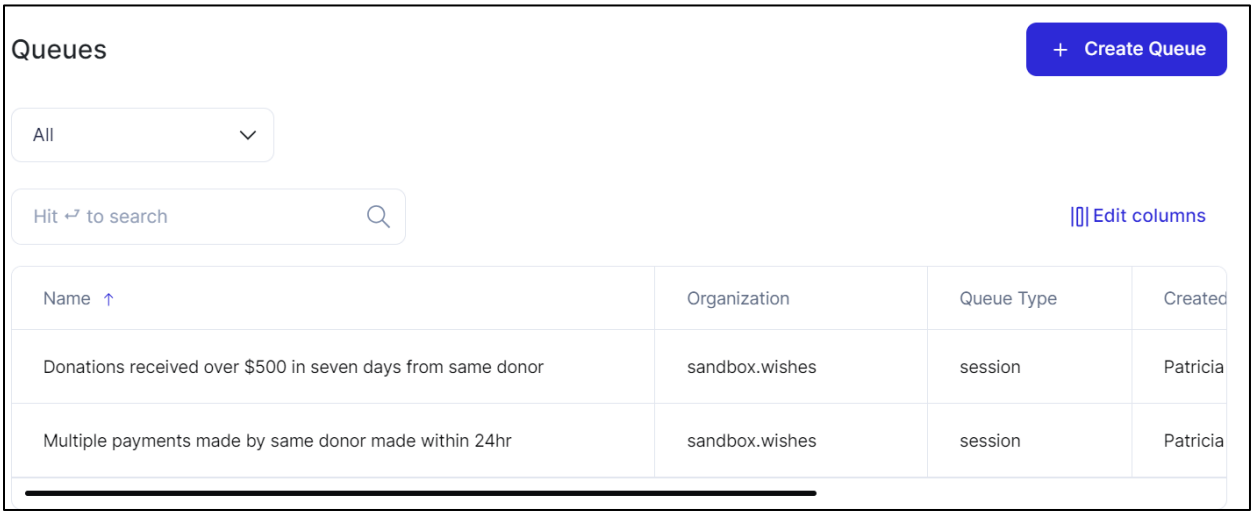




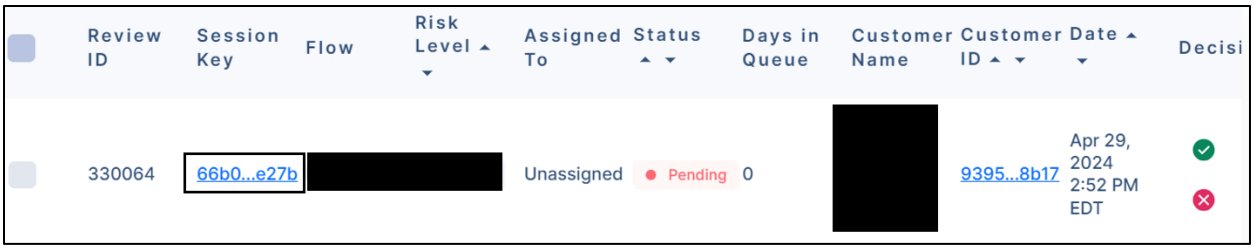
9.3. How to Investigate a Session

Once logged into Sardine, the Analyst will select “Alert Queues” on the left side of the dashboard.

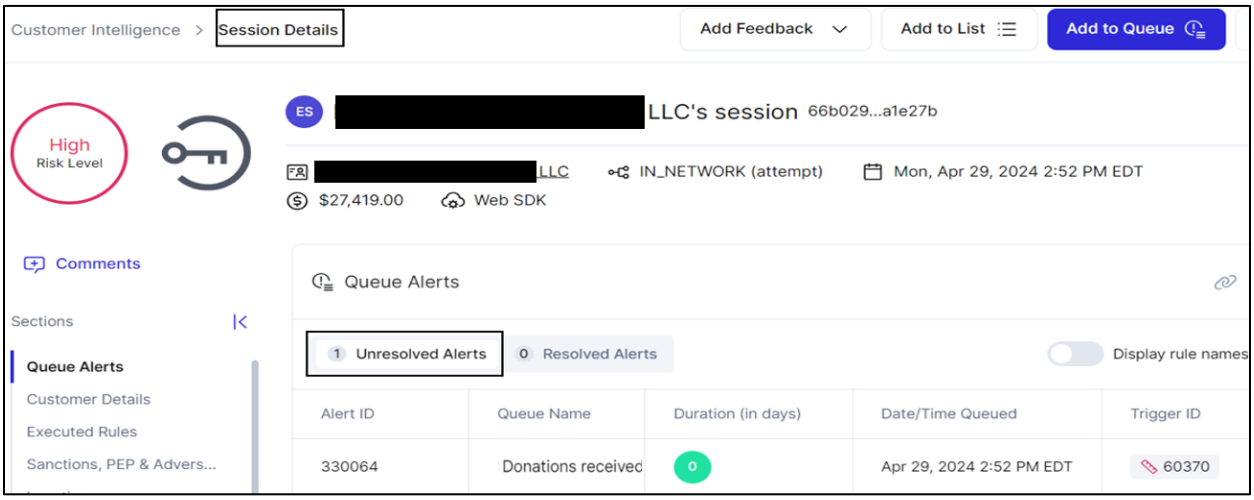
The Alerts page is the first step in the workflow process. Here the Analyst will see all the queues that have alerts still outstanding.



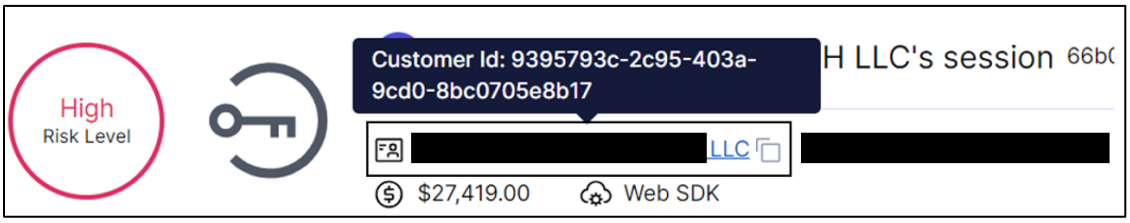
Click in the queue that has an unresolved alert. Select a Session Key link.



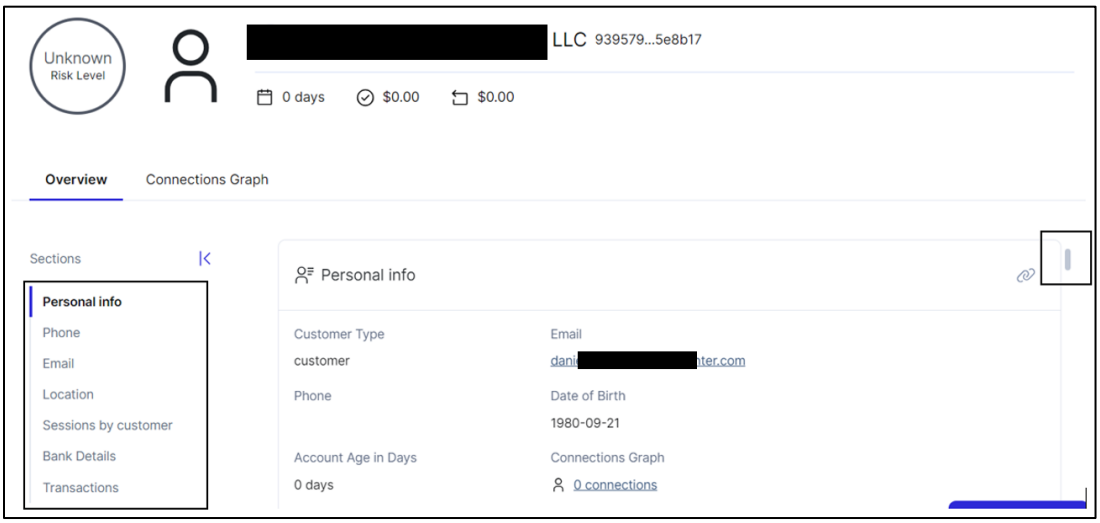
From the Session Details page, start the investigation of unresolved alert.



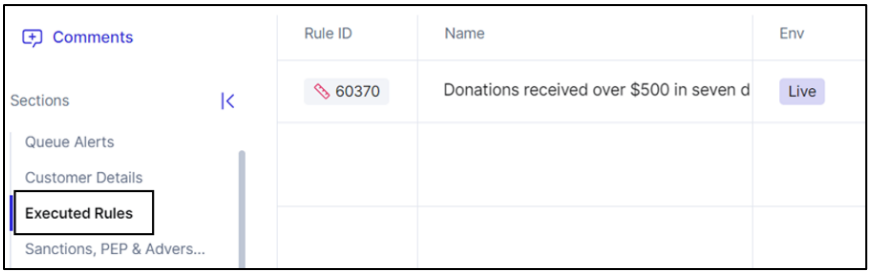
Click on Customer ID to gather information on the customer.



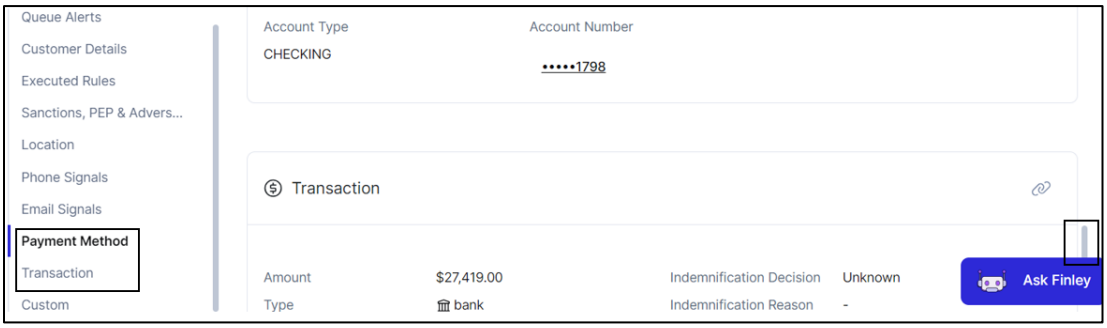
Scroll down and review the information detailed about the customer, such as location, email address, transactions attempted and completed, etc…



Return to the Session page and scroll down and review the rules that were triggered.



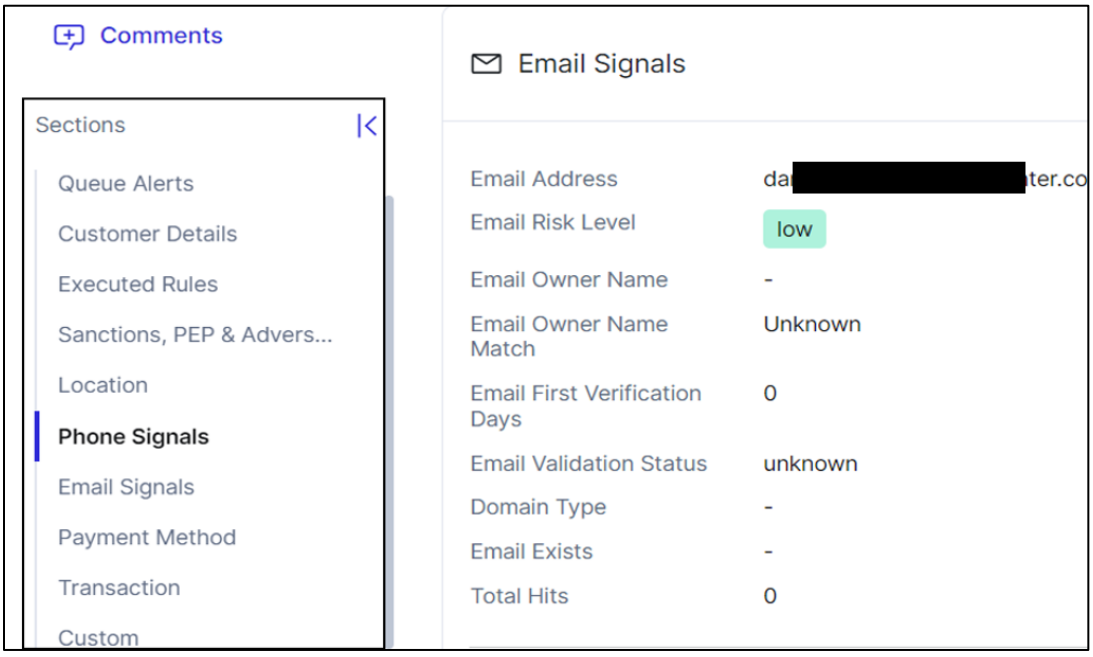
Scroll down on the left and review the transaction details and select payment method.



Review the details regarding the counterparty of the transaction.

XX

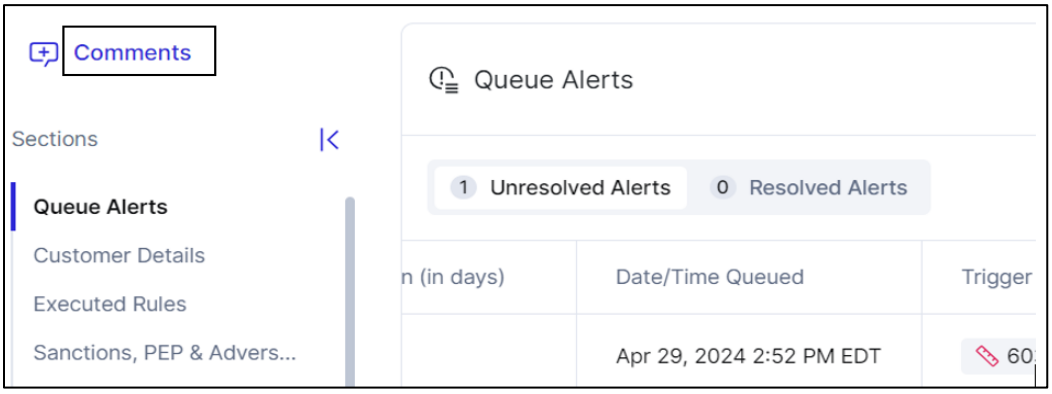
Make sure to review all the sections on the left that have not been examined.



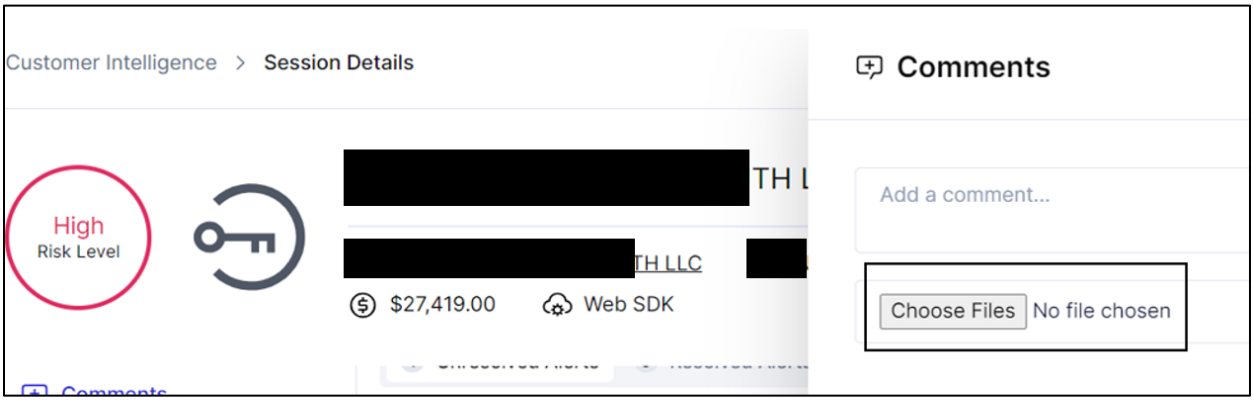
9.4. How to Resolve an Alert

Once the analyst completes the review/investigation of the alert, it must be resolved. There are three options to resolve an alert: *Approve, Decline, and Unsure.*

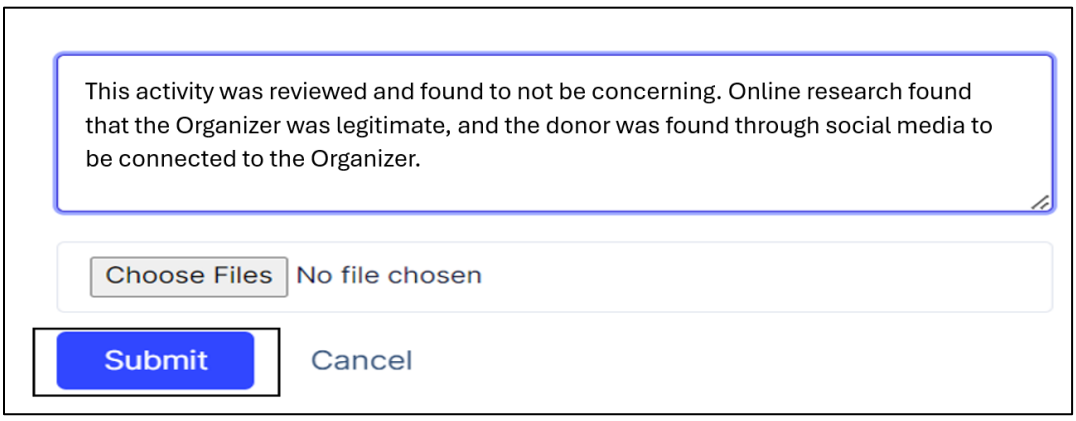
Once the investigation is complete, click on Comments.



Upload any narrative and supporting documentation found during the review.

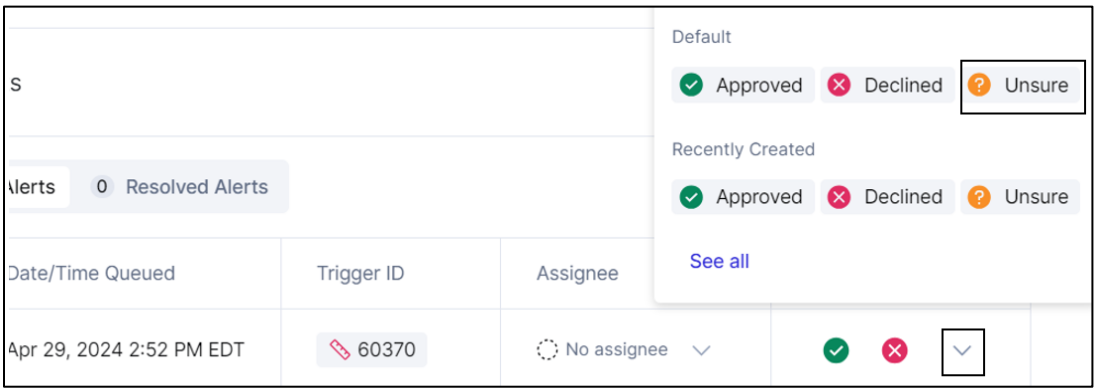


Add a comment to explain disposition.

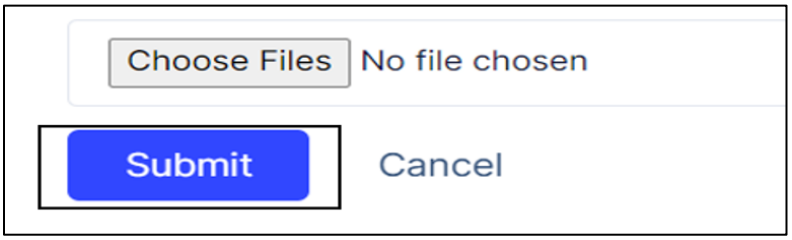


If the alert is being closed with no unusual activity suspected, click on the green check mark for "Approve."

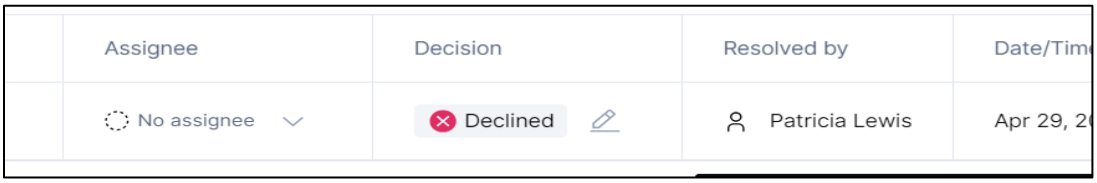
If potentially unusual activity is found and notated on account, click on the down arrow, and choose the option "Unsure."



Once the alert has been reviewed by the CCO, the final disposition will be entered in Sardine. If unusual activity is found, the IR form will be attached to the session via the Comments option.



If an IR form is submitted to the CCO (and then bank partner), the alert will be declined.



If, after a second review, no unusual activity is found, no IR form will be completed, and the alert will be changed from *Unsure* to *Approve*.

	Assignee	Decision	Resolved by
	No assignee	Approved	Patricia Lewis

10. Appendix B

Incident Report Template

INCIDENT REPORT	
Date Reported:	Name of Bank Partner:
Name and Address of Applicant:	**Account number and Date of Application:**
Dollar Amount Requested or Obtained:	**Amount of Financial Loss:** (If applicable)
Name of Suspect: (If identified)	**Are there any application(s) linked to application? Yes: ___ or No___** **If yes, have you provided all relevant details for linked application(s) below?** **Yes: ___ or No___**
***PLEASE BE AS DETAILED AS POSSIBLE IN THE NARRATIVE AND ATTACH ALL SUPPORTING DOCUMENTATION.*	
Submitted By: **Submitted Date:** **Telephone:**	X Employee Signature
FOR BSA USE ONLY: **Approved By:** **Determination Date:**	X Employee Signature

12. Appendix C

Watchlist

Customer ID	Name	Type of Customer (Organizer or Donor)	Date Placed on Watchlist	Reason for Monitoring	Date/Reason for Removal

13. Revision History

The following chart reflects the version of the policy, the source of the changes, a summary of significant changes, who authorized the changes, and when the changes were approved.

Version	Changes by	Authorized by	Description of Change	Date Approved
1.0	Ankura Consulting	CCO	Policy Creation	