Knowledge Article

Sanction Screening

What is Sanction Screening?

Sanction screening is a process used to identify and mitigate risk associated with doing business with sanctioned entities. These entities can be individuals, organizations, or even countries that have been penalized by governments or international bodies for violating regulations or international law.

The screening involves checking a party (customer, business partner, etc.) against comprehensive lists of sanctioned entities. These lists are constantly updated and can include millions of names, making manual checks impractical. Sanction screening software automates this process, streamlining compliance efforts. The sanction screening process is used to discount the alerts generated against the onboarding customer in Safe watch. Sanction screening involves comparing customer information, such as names, addresses, and identification numbers, against various sanction lists.

Why is Sanction Screening Used?

There are several key reasons why sanction screening is used:

- **Compliance with Regulations:** Many industries, especially financial institutions, are legally obligated to conduct sanction screening. Failing to do so can result in hefty fines and even criminal charges.
- **Preventative Measure:** Sanction screening helps organizations avoid doing business with sanctioned entities. This protects them from reputational damage, potential financial losses, and legal repercussions.
- **Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF):** Sanction screening is a crucial component of AML and CTF efforts. By identifying sanctioned entities, organizations can help prevent criminals and terrorists from using the financial system for illicit activities.

Where is Sanction Screening Used?

Sanction screening is most commonly used in the following sectors:

- **Financial Institutions:** Banks, insurance companies, and other financial institutions are at the forefront of sanction screening due to the high volume of transactions they handle.
- **Trade and Shipping:** Businesses involved in international trade need to ensure they are not doing business with sanctioned countries or entities.
- **Healthcare:** Healthcare providers may use sanction screening to comply with regulations related to certain programs.
- **High-Risk Industries:** Any industry with a high risk of money laundering or other financial crimes may benefit from implementing sanction screening.

Sanction screening is being done in 7 processes in RPA, Namely:

1. Sanction Screening for Customer Onboarding
2. Home Remittance Alerts Discounting (Unstructured)

3. Home Remittance Alerts Discounting (Structured)
4. Sanction Screening CTL
5. Sanction Screening CAS
6. Sanction Screening BB
7. RFI COC Automation

Sanction Screening CTL for Customer Onboarding

Process Overview

The Business Unit selects the generated alerts on First in First out (FIFO) real time basis form Safe Watch. Alerts will be sorted based on time stamp. The main purpose of this activity to screen the customer's name form sanction list to avoid the regulatory breach, financial loss and reputational Risk. Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

To identify potential sanctions violations, analysts begin by logging into Safe Watch on the 177 server. They then access the Detection Manager by selecting the Search icon. Within Detection Manager, specific filters are applied to identify new, unreviewed detections within the CTL Zone that may contain hidden clean detections or require a four-eyes review process.

The identified detections will be displayed on screen. If there are multiple alerts associated with a single detection ID, the analyst will select the specific detection for review by clicking on its ID. This will display a list of individual alerts tied to the detection. Each alert can be reviewed by clicking on it, revealing its details in two sections: Structured and Unstructured data.

The analyst will then focus on the Structured Record tab on the left side of the screen. On the right side, details of the potentially sanctioned person will be displayed. Here, the analyst will compare the information in the Structured Record with the provided sanction list.

If there is no match between the customer and the reported violation person, the analyst will document this by entering a comment in the designated box. Following the comment, they will then release the alert using the Release Button (for Level 1 users). However, if a match is found, the analyst will again document the situation with a comment before taking action to block the alert at Level 1 using the Block Button.

Post RPA Workflow

The bot automates the process of reviewing sanction alerts within Safe Watch. It first logs in and selects the search function. On the Detection Manager screen, it filters for specific criteria like open alerts, new status, and a specific zone. Once detections appear, the bot sorts them by creation date and selects them by ID. This triggers the display of associated alerts. The bot then navigates to the customer record for each alert and compares the structured record details (CNIC, Father Name, etc.) with the sanction list. Since these details might have different names in the system, the bot references a shared Excel file maintained by the business to identify all potential matches. The bot then checks the Reported Violation Person

Database for matching information on these parameters. Finally, depending on the match outcome, the bot takes action: closing alerts with comments for no matches (using pre-defined comments) or blocking accounts with comments for matches (also using pre-defined comments). Notably, if an alert requires manual review by a Level 1 Compliance Analyst, the bot won't add comments and will leave the detection open for further investigation. In all cases, the bot generates a real-time report on released/reviewed alerts within a shared folder.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening CTL for Customer Onboarding.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

Sanction Screening CAS for Customer Onboarding

Process Overview

The Business Unit selects the generated alerts on First in First out (FIFO) real time basis form Safe Watch. Alerts will be sorted based on time stamp. The main purpose of this activity to screen the customer's name form sanction list to avoid the regulatory breach, financial loss and reputational Risk. Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

Transaction discounting involves analysts using the SafeWatch system to identify potential sanctions violations. The process starts with the analyst logging in and using the Search icon. On the Detection Manager Screen, they'll select specific options like the "DB Scanner" application, alerts marked as "Open" and "Hidden Clean," "4 eyes detections," "New" status, and the "CAS Zone." This generates detections on the screen. The analyst then reviews each detection by selecting its ID and clicking on "Structured Record." An alert is created for each detection, and the analyst compares the structured record with the sanction list displayed on the right. If there's no match between the highlighted field value and the Reported Violation Person, the analyst enters comments and releases the alert at Level 1. Conversely, if a match is found, they enter comments and block the alert at Level 1.

Post RPA Workflow

The bot automates the review process for potential sanction hits within Safe Watch. It starts by logging in and selecting the search function. On the Detection Manager screen, it filters for open alerts, hidden clean detections, requiring a 4-eyes review, and focusing on new detections within the CAS Zone. Identified detections are reviewed by clicking on their ID and accessing the structured record. The bot then compares information from the record with a sanctions list displayed alongside. Since parameter names might differ, the business maintains an Excel sheet with synonyms in a shared folder. Additionally, the business provides a separate list of unique identifiers via email after updates. The bot

accesses these files and compares specific details (CNIC, Father Name, Nationality, Year of Birth) against the Reported Violation Person Database.

Depending on the match, the bot takes action:

- If no match is found, it closes the alert with a comment and releases it.
- If a match is found, it blocks the account and adds a comment.

For discounted alerts (those not requiring blocking):

- If all sub-alerts under a detection ID fall under rule-based discounting, the bot adds comments to each sub-alert and closes them. It leaves the main detection ID open for L1 review (human analyst).
- If any sub-alert requires manual review (by L1), the bot doesn't add comments and leaves the entire detection ID open for L1 review. The L1 analyst will then provide the final comment.

Finally, the bot generates a real-time report on reviewed/released alerts within a shared folder.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening CAS for Customer Onboarding.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

Sanction Screening Branchless/Konnect for Customer Onboarding

Process Overview

The Business Unit selects the generated alerts on First in First out (FIFO) real time basis form Safe Watch. Alerts will be sorted based on time stamp. The main purpose of this activity to screen the customer's name form sanction list to avoid the regulatory breach, financial loss and reputational Risk. Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

Transaction discounting involves analysts reviewing potential sanctions hits within the Safe Watch system. The analyst first logs in to Safe Watch on the 177 server. Using the Detection Manager search function, they filter for specific criteria such as new alerts, hidden clean detections, and "4 eyes" detections (requiring double verification). The Branchless Zone filter narrows the search further.

Identified detections display on screen. The analyst selects a detection by clicking its ID, revealing a list of individual alerts. They review each alert's details presented in two tabs: Structured Record and Unstructured. The Structured Record tab displays the details being screened against sanction lists. The

analyst compares these details, particularly highlighted fields, with the "Reported Violation Person" on the sanction list.

Using a rulebook with four parameters (CNIC, Father Name, Nationality, and Year of Birth), the analyst decides whether to discount the alert. If there's no match across all four parameters, they comment with "False positive - No positive match found" and release the alert (Level 1 user). Conversely, if a match is found, they comment with the reason for blocking (e.g., "CNIC match with Proscribed Individuals") and then block the alert at Level 1.

Post RPA Workflow

The BOT automates the process of reviewing potential sanction matches within the Safe Watch system. It begins by logging in and navigating to the "Detection Manager" screen. There, the BOT selects specific criteria for filtering detections, including searching for new, unreviewed alerts with hidden clean detections and requiring a four-eyes review process.

Once detections appear, the BOT prioritizes them by creation date and selects them by ID. This triggers the display of associated alerts. For each alert, the BOT reviews the customer record details ("Structured Record") against the provided sanction list. Since naming conventions for key parameters (CNIC, Father Name, etc.) can vary, the BOT references a business-maintained Excel file ("Unique Identifier") that maps these variations. This file is updated and shared with the RPA team for continuous improvement.

The BOT then compares the customer information against the "Reported Violation Person Database" using the same parameters (CNIC, Father Name, Nationality, Year of Birth). Based on the comparison, the BOT takes action:

- If no match is found, the BOT closes the alert with a comment (referencing a specific document) and releases it.
- If a match is found, the BOT blocks the account, adds a comment (referencing a specific document), and leaves the detection open for further manual review by a Level 1 Compliance Analyst. This allows the analyst to review all relevant information before finalizing the case.

Finally, the BOT generates a real-time report summarizing the alerts it has reviewed and their outcomes (released or blocked) which is then stored in a shared folder.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening Konnect for Customer Onboarding.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

Sanction Screening for Customer Onboarding

Process Overview

The Business Unit selects the generated alerts on First in First out (FIFO) real time basis form Safe Watch. Alerts will be sorted based on time stamp. The main purpose of this activity to screen the customer's name form sanction list to avoid the regulatory breach, financial loss and reputational Risk. Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

To investigate potential sanctions violations, analysts will first log in to Safe Watch and select the Search icon. This opens the Detection Manager screen. Here, they'll refine their search by choosing "MQ Connector" under Application, "New" for Status, and ticking boxes for "Contains opened alerts" and "Hidden Clean Detection." Additionally, they'll select "4 eye detection" and specify the "EQ-Mysis Zone." Matching detections will then appear on the screen.

Analysts will delve deeper by clicking on a specific detection's ID and then "Structured Record" for review. This generates an alert tied to the detection. They'll meticulously compare each alert, one by one, with the corresponding sanction list displayed on the right side. The key is to match the yellow highlighted field value within the alert with the "Reported Violation Person" on the sanction list. If there's no match, the analyst will document their findings in the comments box and "Release at Level 1" to close the alert. Conversely, a confirmed match triggers an "Block" action at Level 1, again accompanied by explanatory comments.

Post RPA Workflow

This process automates sanction screening using a bot (BOT). Here's how it works:

The BOT logs into Safe Watch and selects the search icon. It then filters detections based on specific criteria within the Detection Manager Screen: application (MQ Connector), new status, containing opened alerts, including hidden clean detections, requiring 4-eye review, and focusing on the EQ-MISUS Zone. Detected alerts appear on screen. The BOT selects each alert by ID and clicks on "Structured Record" for review. It then generates an alert for each Detection ID and meticulously compares the structured record with the sanction list displayed alongside. Since data may have different names across systems, a business-maintained Excel file stores alternative names for parameters. This file is updated with a unique identifier list and emailed to the RPA team. The BOT accesses this file and compares the following parameters with a Reported Violation Person Database: CNIC, Father Name, Nationality, and Year of Birth. If the shared folder containing the unique identifier list is unavailable, the BOT sends an email notification and halts the process. If no match is found in the database, the BOT closes the alert with a comment in the designated box and clicks "Release."

- **Match:** If a match is found, the BOT blocks the account, adds comments, and follows pre-defined business logic (specified elsewhere) to filter remaining alerts. Based on this logic:
- **Discount:** The BOT adds comments and closes the alert using the "Release" button.

- **Partial Match with Manual Review:** If any sub-alert requires manual review, no comments are added. For sub-alerts following rule-based discounting, comments are updated, but no final comment is added to the Detection ID. This ensures L1 compliance analysts can review the entire Detection ID.
- **Block:** The BOT blocks the alert with comments.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening MYSIS for Customer Onboarding.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

RFI - COC Automation

Process Overview

Sanction screening is a crucial step in the customer onboarding process, acting as a vital shield against financial crime and reputational risk. It involves checking individuals and entities against comprehensive sanction lists issued by governments and international organizations. Home Remittance Service enables remitters to send money from abroad to Pakistan instantly, conveniently, and safely through the legal banking channels. Remittance Alerts Discounting (RFI Cash over the Counter-COC Process for Sanction screening) is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

A. Report Generation:

The alerts list process involves generating a report of pending alerts within SafeWatch. You can specify a date range and download the report in CSV format.

Violation per List (2014): This step focuses on violations identified against a specific blacklist (e.g., AML HOK Black List) with a particular version (e.g., dated September 18, 2014). The report format is Excel. Similar steps are repeated for violations against another blacklist (e.g., World Check Remit home sanction list) dated May 22, 2019.

B. Report Downloading & Data Massaging:

Downloaded reports require data manipulation to identify relevant information. Filtering helps exclude transactions not related to SafeWatch and MQ connector activities. Duplicate entries are removed, and unnecessary columns are deleted. New columns are added to capture details like "Reference No." and "MOT (Mode of Transaction)". Based on comments within the report, transactions are categorized as

requiring details for either the remitter or beneficiary. Missing details are potentially identified by checking comments and SafeWatch's "Text" column for clues. The process is repeated for reports generated in step A, focusing on transactions not related to SafeWatch and MQ connector activities.

C. Excel File Uploading in COTC:

The analyst logs in to the COTC data insertion system and uploads the prepared Excel file (named "COC [current date]"). Upon submission, the system processes the file, and a completion message is displayed. An email containing the uploaded file is sent to the "[email address removed]" team for further action.

D. Alert Discounting:

The analyst receives an email from a branch containing a reference number related to a potential sanction match. SafeWatch's detection manager is accessed to search for the reference number. If not found, a broader search with wildcards is attempted. Individual alerts are reviewed, comparing information from the branch email and the corresponding sanction list entry in SafeWatch. Discrepancies in year of birth or nationality/place of birth might indicate a false positive, prompting comments and potential release of the transaction. If a clear match is identified, further investigation might be required.

Post RPA Workflow

This process automates the download and processing of reports generated by the SafeWatch system for sanction screening. It operates from Monday to Saturday, starting at 8:30 am.

Report Generation:

- The bot logs in to SafeWatch and retrieves two reports:
    - **Alert List:** This report identifies pending alerts within a specific date range (previous business day to current day) and is downloaded in CSV format.
    - **Violation per List:** This report focuses on violations against specific blacklists (e.g., AML HOK Black List for 2014 and World Check Remit home sanction list for 2019). The bot downloads these reports in Excel format, specifying the relevant blacklist version for each.

Data Processing:

- Downloaded reports undergo data manipulation to extract relevant information. This involves:
    - Filtering out transactions unrelated to SafeWatch API and MQ connector activities.
    - Removing duplicate entries and unnecessary columns.
    - Adding new columns for details like "Reference No." and "MOT (Mode of Transaction)".
    - Categorizing transactions based on comments within the report, indicating if details are required for the remitter or beneficiary.
    - Identifying missing details by checking comments and SafeWatch's "Text" column.

Excel File Uploading and Alerting:

- The processed data is uploaded to the COTC data insertion system, named with the current date and time (e.g., "COC [current date & time]").
- Upon successful upload, a screenshot is captured and emailed to the home remittance group along with the uploaded file.

Alert Discounting:

- When an email notification arrives from a branch regarding a potential sanction match, the bot performs the following actions:
    - Extracts the reference number from the email.
    - Searches for the reference number in SafeWatch, expanding the search with wildcards if not found initially.
    - Analyzes individual alerts by comparing information from the branch email and the corresponding sanction list entry in SafeWatch.
    - Discrepancies in year of birth or nationality might trigger comments like "False Positive" and potentially clear the transaction.
    - If a clear match persists, the alert is flagged for manual review and forwarded to the home remittance group for further investigation.
    - A special verification process is applied for beneficiaries younger than 18 years old, requiring manual review before discounting.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening for remittance alert discounting when onboarding customers.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

Sanction Screening for Home Remittance Transaction Alert (Un-Structured)

Process Overview

Sanction screening is a crucial step in the customer onboarding process, acting as a vital shield against financial crime and reputational risk. It involves checking individuals and entities against comprehensive sanction lists issued by governments and international organizations. Home Remittance Service enables remitters to send money from abroad to Pakistan instantly, conveniently, and safely through the legal banking channels. Remittance Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

Alerts generated on remittances are either on remitter or beneficiary. If an alert is generated on remitter, analyst reviews information and discounts the alerts based on available discounting factors i.e.; nationality & date of birth. There are 03 types of transactions for beneficiary that are discounted under home remittance, either COC, own bank account holder or other bank account holder. For own bank account holder or other bank account holder, alerts are discounted as own account holders are already covered under delta review whereas other bank account holder screening is responsibility of beneficiary's bank as per SBP clarification letter. For the hits against the COC beneficiary names, information is reviewed, and alert is discounted based on available discounting factors. Where discounting factors are unavailable, RFI is raised to the relevant business unit for provision of information. Alert is discounted once information is received, and the transaction is either blocked or released for payment after L2 review.

Post RPA Workflow

Alert Review Process:

1. The bot searches for open alerts within a specific date range, focusing on SafeWatch API activities.
2. It analyzes each alert by comparing information from the unstructured record with the corresponding sanction list entry. Information fields are identified by alphanumeric codes (e.g., :50K: for remitter information).
3. The bot reads a shared folder for updates on unique identifiers like Date of Birth and Nationality used for matching against the sanction list.
4. Alerts triggered for reasons other than Remitter/Beneficiary name are sent for manual review.

Remitter/Ordering Customer Review:

- If the Remitter's nationality isn't Pakistan, the alert is sent for manual review.
- If the alert category on the sanction list is "Country," the bot automatically discounts the transaction with a comment explaining the mismatch (individual vs. country).
- The bot compares the Remitter with a provided list and sends alerts for matches to manual review.
- Otherwise, the bot discounts the alert based on predefined rules.

Age Verification:

- The bot extracts the Remitter's year of birth from a specific field, considering various date formats.
- Alerts for individuals under 18 are sent for manual review.

Beneficiary Review:

- If the alert is on the Beneficiary, the bot checks their nationality. Alerts for Pakistani, Afghani, or unknown nationalities are sent for manual review.

- For Cash Over Counter transactions, the bot auto-discounts if the nationality/place of birth on the sanction list doesn't match specific criteria (Pakistani, Afghani, or unknown). It also discounts if the category is "Group."
- For Own Account Remittances (HBL account holders), the bot identifies them by bank details and auto-discounts with a comment about further screening.
- For Other Bank Account Remittances, the bot auto-discounts with a comment indicating screening responsibility lies with the third-party bank.

Outcomes:

- The bot assigns reviewed alerts to a specific group or discounts them based on matching or mismatching criteria.
- Comments are added to explain the actions taken.
- A productivity report of each reviewed alert is saved in a shared folder.

Systems and Tools Used

Below listed system and tools will be involve in the automation of the Sanction Screening for remittance alert discounting when onboarding customers.

1. SafeWatch system http://10.200.15.177:9080/AMLUI/SWAF/jsp/login.xhtml
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder

Sanction Screening for Home Remittance Transaction Alert Structured

Process Overview

Sanction screening is a crucial step in the customer onboarding process, acting as a vital shield against financial crime and reputational risk. It involves checking individuals and entities against comprehensive sanction lists issued by governments and international organizations. Home Remittance Service enables remitters to send money from abroad to Pakistan instantly, conveniently, and safely through the legal banking channels. Remittance Alerts Discounting is a process of clearing the hits or matches generated as per predefined parameters of fuzzy matching criterion employed in a name screening solution, SafeWatch.

Pre RPA Workflow

Home remittance alerts are discounted per rule book. There are 03 types of transactions that are discounted under home remittance .

Rules of Discounting for Beneficiary

1.Cash over Counter Remittances (OC)- If the Nationality / Place of Birth on sanction list is other than the below then auto discount the transaction, otherwise refer the alert for manual review:

i. Pakistani
ii. Afghani

iii. No Nationality or No Place of Birth is mentioned.

iv. If the Category on sanction list is " Group" then auto discount the transaction with the comment " False Positive: Individual Vs Group. "

2.For Own Account Remittances **(AC)-** If the beneficiary is HBL account holder, then auto discount the transaction with the comments, **own account holder subject to delta/portfolio screening**.

3. For Other Bank Account Remittances **(IB / BT) -** If the beneficiary is other bank account holder, then auto discount the transaction with the below comments "**Detection on 3rd party bank Beneficiary. Screening responsibility with 3rd Party Bank as per letter sent to SBP and relevant banks, and risk acceptance letter by business".**

An analyst in the SafeWatch system follows a specific process to review and resolve potential sanction matches. Here's a breakdown of the steps:

1. The analyst logs in to SafeWatch and uses the Search function to identify relevant alerts. They filter for alerts generated by the MQ Connector, focus on unreviewed items, ensure they require double verification (4 eyes detections), and target alerts with a "New" status. From the search results, the analyst selects an alert by clicking its ID. They then choose "Structured Record" for a detailed review. The chosen alert generates a corresponding record. The analyst meticulously compares the details in this record (e.g., Remitter or Beneficiary information) with the sanction list displayed on the SafeWatch screen. The course of action depends on which party triggered the alert (Remitter or Beneficiary) in the "Field Name" section of the record.
   - **Remitter Alert:** If the alert is on the Remitter, the analyst specifically checks the Remitter's birth year and nationality for discrepancies.
   - **Beneficiary Alert:** If the alert is on the Beneficiary, the analyst focuses on yellow highlighted fields to determine if name discounting is possible. In cases where discounting isn't applicable, they can follow the initial search steps (4.1) to locate further relevant alerts.
2. **Finalize Alert Status:** Based on the review, the analyst can take one of three actions:
   - **Discount Alert:** If a discrepancy is found (e.g., birth year mismatch), the alert is discounted.
   - **Mark Pending:** If information is missing or incomplete, the alert is marked as pending for further investigation.
   - **Block Alert:** If all criteria for a true sanction match are met, the alert is blocked.
3. **Document and Close:** After updating the alert with comments explaining the chosen action, the analyst moves it to Level 2 (L2) for final closure. This ensures a second review and confirms the resolution.

Post RPA Workflow

The bot streamlines sanction screening tasks within SafeWatch. Daily, the BOT logs in and selects alerts based on specific criteria: MQ Connector application, open alerts with "4-eyes detections" and "New" status. It then analyzes each alert by reviewing the corresponding structured record and matching it with the sanction list.

To make informed decisions, the BOT accesses a shared folder (updated by the business team) containing the latest rulebook and a list of unique identifiers like Date of Birth and Nationality

from the sanction list. Based on the "Field Name" triggering the alert (Remitter or Beneficiary), the BOT takes specific actions:

- **Remitter Alert:** It checks the Remitter's details (Birth Year or nationality) and can discount (clear), mark pending (incomplete information), or block the alert (all blocking criteria met). Comments are added depending on the action (e.g., "Identifiers matched, please Review" for manual review). The updated alert is then moved to Level 2 for closure.
- **Beneficiary Alert:** Depending on the transaction type:
  - **Cash Over Counter Remittances (OC):** It auto-discounts if Nationality/Place of Birth doesn't match specific criteria, refers for manual review if there's a match, or auto-discounts for "Group" Category with a specific comment.
  - **Own Account Remittances (AC):** It auto-discounts for HBL account holders.
  - **Other Bank Account Remittances (IB/BT):** It auto-discounts with a comment referencing the third-party bank's screening responsibility.

The BOT saves a productivity report for each reviewed alert and handles Detection IDs with multiple sub-alerts by adding comments based on the rulebook (except for those requiring manual review). This automation improves efficiency by processing alerts systematically, reducing manual work, and ensuring adherence to screening guidelines.

Systems and Tools

Below listed system and tools will be involved in the automation of the Sanctions Screening for Home Remittance Alerts (Unstructured).

1. SafeWatch system
2. Microsoft Excel
3. Microsoft Outlook
4. Shared Folder