w­­­­­

|  |  |
| --- | --- |
|  |  |



**Solution Design**

**Document**

Table of Contents

[I. Purpose 3](#_Toc83027293)

[II. Automated process details 4](#_Toc83027296)

[2 Runtime guide 5](#_Toc83027297)

[2.1 Architectural structure of the Master Project 5](#_Toc83027298)

[2.2 Master Project Runtime Details 7](#_Toc83027299)

[3 Other Details 11](#_Toc83027303)

[Debugging Tips 11](#_Toc83027305)

[Post UAT Specifications 11](#_Toc83027306)

[4 Glossary 11](#_Toc83027307)

Creation Date: 06.12.2023

Created By: Horatiu Deac

# Purpose



Overview

The Fraud Detection Automation Process is a strategic initiative aimed at empowering the Fraud Team to operate more efficiently and effectively through the utilization of UiPath automation tools. By centralizing account details and streamlining actions within the UiPath Action Center, this process enhances the team's capabilities in fraud detection, investigation, and response. The ultimate goal is to deliver superior customer experiences, ensure regulatory compliance, and optimize resource utilization.

Purpose

1. Centralized Data Management

The primary purpose of the Fraud Detection Automation Process is to centralize the management of account details, enabling the Fraud Team to access comprehensive information from various sources in one unified platform. This centralized approach significantly reduces the time and effort required for data gathering, allowing agents to focus on critical tasks related to fraud detection.

2. Streamlined Decision-Making

By automating the collection and presentation of account information, the process facilitates more informed decision-making within the Fraud Team. The UiPath Action Center Form serves as a streamlined interface where executives can easily review data and select appropriate actions. This ensures that decisions are consistent, well-informed, and align with established fraud detection strategies.

3. Enhanced Efficiency in Investigations

The automation process expedites investigations by retrieving Yoda information for the main account, details for linked accounts, and relevant data points. This comprehensive data set empowers the Fraud Team to conduct thorough investigations with minimal manual effort. As a result, the team can respond quickly to potential fraud cases, minimizing the impact on customers and the organization.

4. Improved Customer Experience

Efficiency in fraud detection directly translates to an improved customer experience. By leveraging automation to expedite investigations and responses, the Fraud Team can proactively address potential issues, mitigate risks, and provide a seamless and secure experience for customers.

5. Regulatory Compliance

The Fraud Detection Automation Process is designed to ensure compliance with regulatory standards and requirements. By centralizing data, documenting actions, and providing transparency in the decision-making process, the automation supports the Fraud Team in adhering to regulatory guidelines and maintaining the highest standards of integrity and security.

6. Optimal Resource Utilization

Automation optimizes resource utilization by reducing manual, repetitive tasks. The Fraud Team can allocate their time more strategically, focusing on complex analyses and decision-making rather than routine data gathering. This results in a more efficient use of skilled resources within the team.

In summary, the purpose of the Fraud Detection Automation Process is to revolutionize the way the Fraud Team operates, providing them with the tools and capabilities needed to detect and respond to fraud in a more agile, informed, and customer-centric manner. Through centralized data management, streamlined decision-making, and enhanced efficiency, this automation process contributes to the overall success of fraud detection efforts within the organization.

# Automated process details

|  |  |
| --- | --- |
| Item | Description |
| Master Project Name | fraud-detection-performer |
| Process Name in Orchestrator | Fraud\_Detection\_Performer |
| Robot Type | Unattended |
| Orchestrator used? | Yes |
| Queue Based | Yes |
| UiPath version used | 2021.10.8 |
| Slack channels | rpa-fs-automation-alerts |

# Runtime guide

## Architectural structure of the Master Project

1. Information Gathering

The automation process starts by retrieving information from the UiPath queue. This information can be sourced from two primary locations:

FeatureSpace Alerts: Alerts are set within FeatureSpace to identify potential fraud cases.

SelfServe Process: The Fraud Team has the capability to initiate the process by adding a script through the SelfServe process, triggering the Fraud Detection automation.

2. Retrieve Yoda Information for Main Account

Once the information is gathered, the process proceeds to retrieve all relevant details related to the main account using the Yoda system. This step ensures a comprehensive overview of the main account's data.

3. Retrieve Linked Accounts

Following the retrieval of Yoda information, the automation process identifies and retrieves all linked accounts associated with the main account. This step is crucial for a holistic understanding of the account relationships.

4. Retrieve Linked Accounts Data

With the linked accounts identified, the automation process collects detailed data for each linked account. This step aims to provide a comprehensive dataset for analysis.

5. Create Form

A UiPath Action Center Form is dynamically created based on the gathered information. This form serves as a centralized interface for the Fraud Team to review account details and select actions to be taken.

6. Check Flag Settings

The automation process checks the settings configured by agents to flag specific accounts. This step ensures that the Fraud Team's preferences and criteria for flagging accounts are considered in the decision-making process.

7. Add Flag and Client Note

Based on the agents' settings, the process adds a specific flag to the account and includes a client note for reference. This ensures that flagged accounts are easily identifiable, and relevant information is documented for future reviews.

Benefits

Efficiency: Centralized data gathering and review in one platform streamline the workflow, saving time for the Fraud Team.

Customer Experience: By expediting the fraud detection process, the team can respond promptly, contributing to a better overall customer experience.

Regulatory Compliance: The automation process ensures that flagged accounts are handled in accordance with regulatory requirements, reducing the risk of non-compliance.

## Master Project Runtime Details

|  |  |
| --- | --- |
| ITEM NAME | DESCRIPTION |
| Production environment details | *TBD* |
| Prerequisites to run | *Access to Yoda* |
| Input Data | *Transaction item with all the arguments filled*  ***Example:***  Specific Data: Object  Account\_ID: 45850520  Brand: PP  Origin: TMX |
| Expected output | ***ProcessRunOutput:*** *Account actioned successfully, action:fraudPromotionsAbuseLowRisk* |
| How to start the automated process | *New Transaction item available in Queue* |
| Reporting | *N/A* |
| How is Orchestrator used? | *The process will be started from orchestrator server* |
| Stored credentials | *Stored in Orchestrator as assets* |
| List of queues names | *Fraud\_Detection* |
| Schedule Details | N/A |
| Multiple Resolutions Supported? | *Yes* |
| Recommended Resolution | *N/A* |

**Project Dependencies (Activities)**

This Automation requires the following Activities:  
 "PPB.Database.Activities": "[1.0.1]",

"PPB.Yoda.Activities": "[1.0.67]",

"UiPath.Form.Activities": "[1.7.1]",

"UiPath.FormActivityLibrary": "[1.7.1]",

"UiPath.Persistence.Activities": "[1.3.1]",

"UiPath.System.Activities": "[21.4.1]",

"UiPath.UIAutomation.Activities": "[21.4.3]",

"UiPath.WebAPI.Activities": "[1.7.0]"   
  
These can all be installed from the “Manage Packages” window in UIPath Studio.

**Project Dependencies (Config)**

* Asset FRAUD\_DW13\_YODA must be present in Orchestrator folder where the process is running.
* Slack bot must be connected to rpa-fs-automation-alerts

# Other Details

### Triggers

*• This process will be triggered from 2 sources:*

*FeatureSpace and SelfServe process. The owner of the FeatureSpace connector is Fraud Team, POC – Robert Kenna*

*Fraud SelfServe process. In order to have queue items from this process Fraud team must add a script file in .txt format on their F: shared drive in any of the Redshift/POD folder. If the Action set by Fraud team is 15 the process will add a queue item with the account to the Fraud Detection queue.*

### Debugging Tips

*• Enter hardcoded customer account data to the specific component in order to perform debugging tasks.*

### Post UAT Specifications

|  |  |
| --- | --- |
| ITEM NAME | DESCRIPTION  Fill in each bolded section - empty fields are not allowed. If the section does not apply to your automation then mark as n/a. |
| Average Handling Time per Transaction | ~ 2 minutes |
| Recommended Number of Robots | 2 |
| Specified Schedule | N/A |

# Glossary

**Master project** - the overall output of the development, containing one or multiple projects that together cover the scope of the robotic process automation. There is a 1 to 1 connection between the Master Project and the Process to be automated (As presented in the PDD).

**Project** - an UiPath Studio project containing one or multiple workflow files. A project can be converted to a package and run independently, covering a particular scope within the master project. Or multiple projects can be converted into one package depending on the aims and restrictions of the automation. The project is used when defining the development and support phase of the automation.

**Package** - the output of compiling one or multiple projects. A package can be deployed on the robot machine and be executed by the robot service. Only one package can be executed at a given time by a robot. The package is used when defining the running phase of the automation.