KYC User Guide

As at April 8, 2024

INTRODUCTION

Jurisdictions across the globe implement Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) regulations to prevent bad actors from evading name verification checks and disguising illegally obtained funds as legitimate income. Following terrorist attacks in Paris and Brussels, which were primarily funded by virtual currencies and prepaid cards with anonymous or fictitious names, government bodies enhanced their current process/regulations to have more control over these payment types. Governments hope these limitations will help prevent future attacks and reduce illegal activity.

The European Union (EU) and the United Kingdom (UK) have enhanced AML/CTF regulations targeting money laundering, terrorism and other emerging threats. The EU's/UK's Fifth Anti-Money Laundering Directive (AMLD5) place increased responsibility on financial entities such as your program manager and its banking partners to implement sufficient controls to capture and mitigate AML risk. The focus of the new regulatory changes is to regulate virtual currencies and prepaid cards, while improving the safeguards for financial transactions to and from high-risk countries. Based on the changes, we are required to implement the necessary controls to verify the name of the payee to prevent the use of anonymous and fictitious names and verify the identity of payees with Know Your Customer (KYC) controls.

As the nature of financial crime evolves, enhancements to AML/CTF regulations offer greater protections for your program manager, their bank partners, their clients and their payees, ensuring that all parties can continue to implement and maintain successful, compliant payment programs.

Use this guide to understand the program manager's AML/CTF procedures:

- Fictitious Name Monitoring
- Address Validation
- KYC Checks

KYC User Guide

TABLE OF CONTENTS

WHAT IS FICTITIOUS NAME MONITORING?

A payee purposely entering bad data to evade name verification requirements usually indicates suspicious activity and is considered an AML/CTF red flag. In online scenarios where the payee is not interacting directly with the financial institution issuing the payment, suspicious activity is more common. Red flags include payees reluctant to provide required legitimate information when redeeming their payment. Instead, they may provide:

- Minimal information (Mister Cook)
- Fictious information (Mickey Mouse)

Financial institutions are obligated by AML/CTF regulations to verify and scrutinize the quality of personal data provided by first-time payees. As a regulated payments provider, the program manager is also required to screen for fictious names. To reduce AML/CTF risk and meet regulatory requirements, the program manager has implemented a third-party name verification solution, Melissa Global Name API, to detect the use of fictious and/or suspicious names.

HOW DOES FICTIOUS NAME MONITORING WORK?

Melissa Global Name API recognizes 650,000+ ethnically-diverse first and last names to verify the data provided by the payee. The Melissa Global Name API monitoring tool integrates seamlessly with the program manager's digital platform to deliver real-time checks during each redemption. As part of the check, full names are parsed into five components (Prefix, First Name, Middle Name, Surname, Suffix) and then fictious data, including vulgar words, fake names and gibberish are identified.

KYC User Guide

FICTIOUS NAME MONITORING USER FLOW

Step 1: The real-time check by Melissa Global Name API seamlessly integrates with the standard redemption process.

If the payee enters complete and valid data, they can expect to proceed to the next step in the redemption flow. However, if the information provided triggers a common fictitious names red flag, the payee receives an error message prompting them to review and confirm their name entry.

Error	Example	Message
Fictitious Name	Mickey Mouse	Please review and confirm your entry for first and last name. Incorrect information could delay access to your payment.
Gibberish	fdsa jkl	
Character Limit Not Met	A	Please enter a First Name greater than 2 characters. Please enter a Last Name greater than 2 characters.
Same First and Last Name	Smith Smith	We're sorry, your First and Last Name cannot match exactly. Please add your middle initial to the First Name Field.

Step 2: The payee will be given another opportunity to provide correct information. If the payee provides a name that results in another error, they will be prompted to complete the KYC process outlined below.

KYC User Guide

WHAT IS ADDRESS VALIDATION?

Address validation is a measure taken to prevent redemption by payees who enter inaccurate / false address information or who are located in comprehensively sanctioned countries (and associated major cities). All addresses entered by payees are cleared through the program managers' third-party address validation solution (Smarty) to ensure the address is valid.

HOW DOES ADDRESS VALIDATION WORK?

Smarty utilizes the United States Postal Service for US addresses and country specific postal service records for international addresses in order to ensure the entered address is accurate. The process for address validation depends, in part, on whether the address is within the US or international.

US Addresses
Payee enters an address which is validated by Smarty. Once validated, the payee is able to redeem their payment.

International Addresses
The payee has three (3) attempts to enter an address that is validated by Smarty. If after the third attempt, Smarty is not able to validate the address entered, the payee will be prompted to go through KYC as outlined below.

WHAT IS THE KNOW YOUR CUSTOMER (KYC) PROCESS?

The Know Your Customer (KYC) process consists of real-time checks of payees who are paid in select currencies on its digital payment platform (prepaiddigitalsolutions.com and custom URLs). Required by regulations and the program manager's banking partners, the threshold-based checks are designed to minimize the risk of the program manager and its clients and partners from being used to facilitate money laundering or other financial crimes.

HOW DOES THE KYC PROCESS WORK?

As outlined above, the payment platform initiates a KYC check whenever a payee:

1. Does not pass fictitious name monitoring or
2. Does not pass international address validation

In addition, KYC is prompted after the payee attempts to redeem a payment that causes their cumulative total payment amount, tracked by their email address, to reach the applicable threshold. (**Note:** See **Threshold Requirements).**

When a fictious name is detected, international addresses cannot be validated, or the KYC threshold is crossed, the payment user journey is preempted by an **Identity Verification** pop-up. To claim their payment (and any future payment), the payee must provide at minimum their full name, primary residential address, and birth date. Depending on the country of residence, the payee may be prompted to enter additional personal identification information such as: National ID number, Tax File Number, Passport Number, etc. (**Note:** Refer to the **Data Sources Table** for details).

KYC User Guide

The payee may choose to provide the required information at the time they are prompted or may opt to return later to provide the information and proceed with the verification process. However, they will not be able to access the funds from the payment that triggered the KYC threshold or future payments until they have provided the information and cleared the KYC check.

Once the payee submits the required information, their identity will be verified and checked against various jurisdictional AML and Sanctions watchlists in real-time. If the payee is cleared, they will continue to the next step of the payment redemption journey to access their funds.

If the KYC check requires further review (e.g., if the system is unable to validate the payee's identity or if the individual's information is a potential match for an AML watchlist), the program manager will work proactively to clear the individual within 5 business days and may reach out to the payee via email as part of the process.

- If we are unable to validate an individual's identity, they will be unable to access the funds from their current payment or any future payments until their account is cleared. They can continue to spend funds that they have already received.
- If the information entered by an individual is a potential watchlist match, they will be unable to access the funds from any current or future payments. ***Any previously earned funds will also be blocked in the case of a potential watchlist match.***

Once an individual is cleared, they can access funds for all current and past payments and can receive and access new payments.

Note: If payees are unable to access their funds after 5 business days, they can reach out to the Customer Support number listed on the payment platform for an update or further guidance.

In the case of a confirmed positive watchlist hit, a block will be placed on all cards associated with the individual and any funds will be returned to the funding account or remitted per the program sponsor's instructions. In cases where an individual's identity cannot be validated, the Account Manager will notify the program sponsor.

KYC User Guide

KYC USER FLOW

Step 1: A payee receives a payment and is presented with an **Identity Verification** request.

Note: Payee must confirm their residential address and input their date of birth (DOB).

Residential Address & DOB Confirmation:

Note: Depending on the country of the residential address, payees may be prompted to enter additional government issued personal identification numbers.

KYC User Guide

Personal Identification Number Confirmation:

Step 2: Payee selects their birthdate from a calendar drop down, confirms their residential address and, if prompted, enters their required personal identification number.

Step 3: Once the payee submits their information, it is verified against various jurisdictional AML and Sanctions watchlists in real-time. There are two reasons a payee may not pass the verification process immediately:

- Unable to Validate
- Potential AML Watchlist Match

Note: The residential address should be updated if incorrect. Failure to provide an accurate primary residential address may cause a KYC failure and delay verification and funds access. Payees must carefully review their address on file and make updates as required.

KYC User Guide

Step 4: In either instance where the payee's information cannot be validated instantly, they are asked to provide additional documentation.

- If using a desktop computer, the payee is prompted to scan a QR code to upload their documents using a mobile device. The QR code will take them to the partner's site titled, **Let's confirm your identity** on their mobile device. The view on the desktop will show each step being performed on mobile and check off each step in the process as completed on mobile.
  Note: To comply with the latest security and identity standards, users will be required to complete this via their mobile device.
- If using a mobile device, after selecting Continue, the user will be automatically directed to the partner's site titled, **Let's confirm your identity.**
  Note: Identification options vary by country.

Desktop Prompts   Mobile Prompts

KYC User Guide

Step 5: The payee follows instructions to select their document and capture an image of their document using their mobile device camera. **Note:** For some identification types (e.g., passport), the payee is only required to capture the front image.
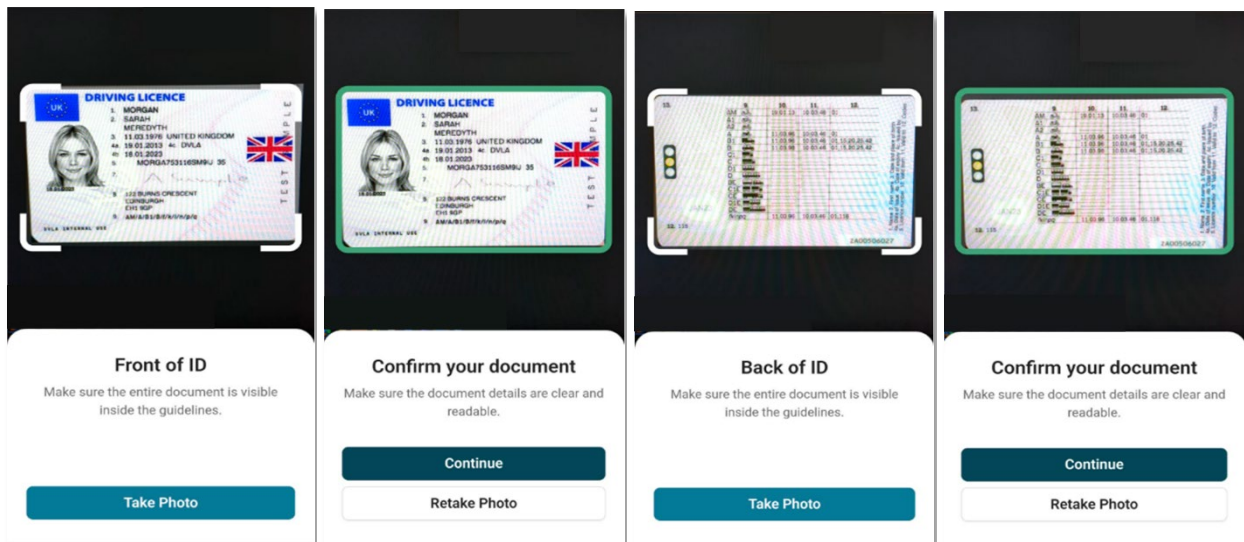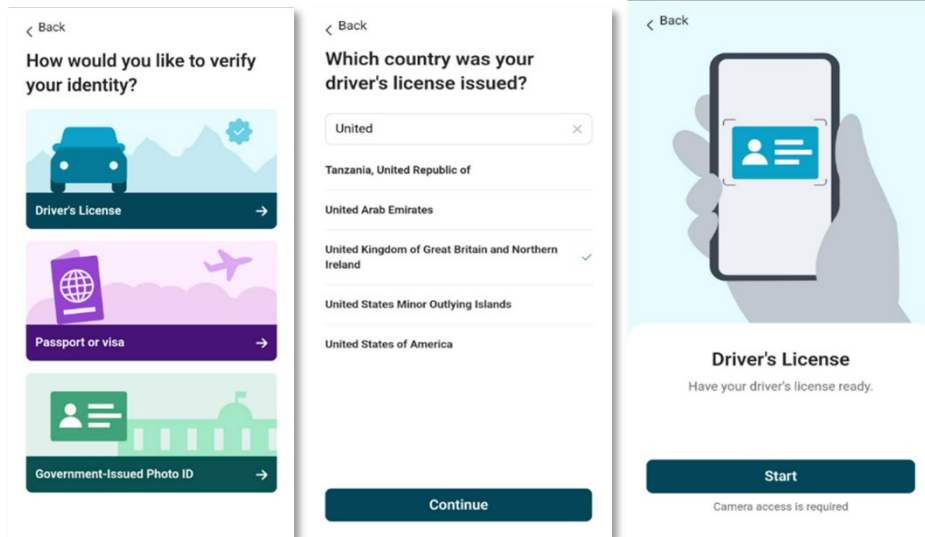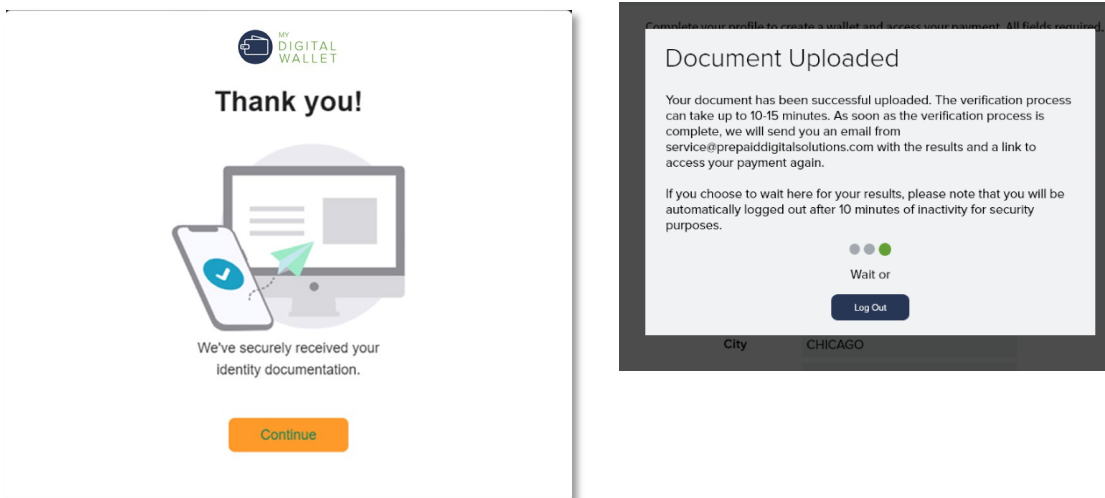
KYC User Guide

Step 6: The payee reviews the images and selects **Submit** to upload the document. Upon submitting, the document is securely transmitted to the partner for verification.
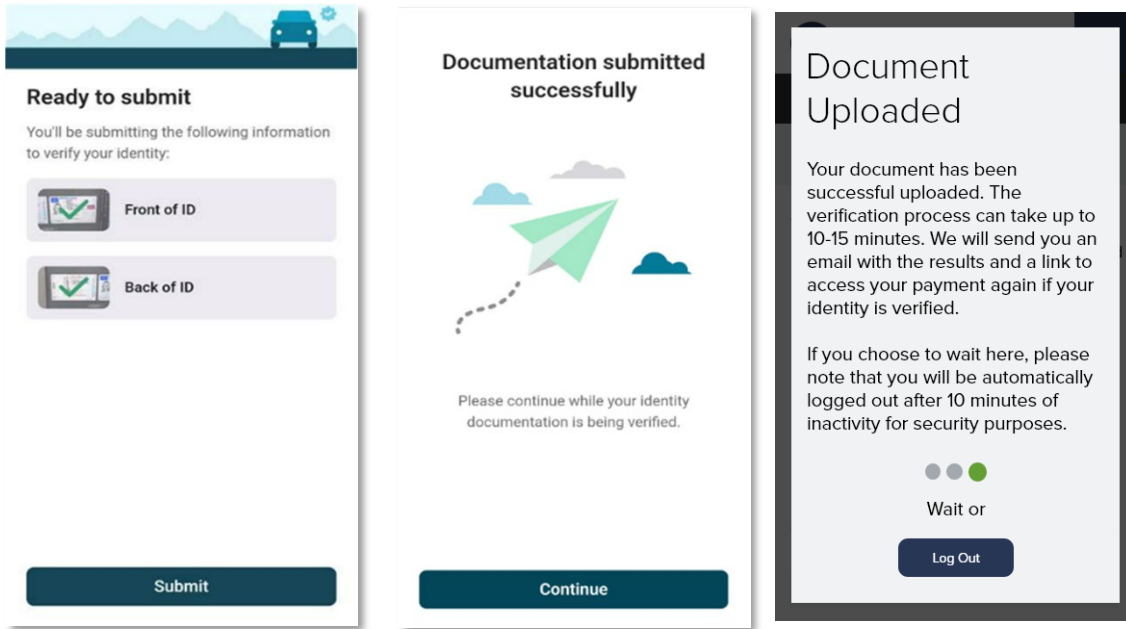
Step 7: The payee is notified that their document has been successfully uploaded and that their verification is in process. Upon completion of their verification, payees will receive an email from **service@prepaiddigitalsolutions.com** with the identity verification results.

- If the payee began the KYC process on a desktop computer, they will be directed on their mobile to return to the open window on the desktop.
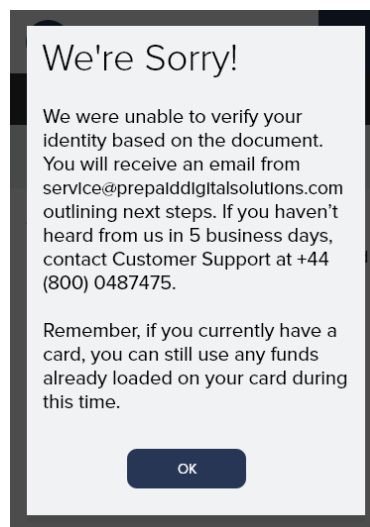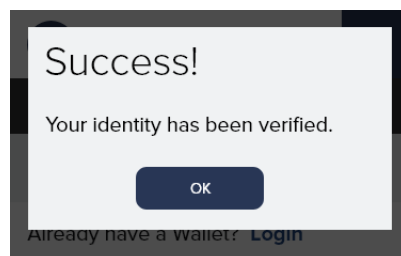
KYC User Guide

Step 8a: Payees will receive an email from **service@prepaiddigitalsolutions.com** with their identity verification results.

- The payee will receive the Identity Verification Complete email (below, left) if the automated process confirms their identity. To access their payment, the payee clicks the **Confirm Your Payment** button in the email or enters their digital token on the payments site.
- The payee will receive the Identity Verification Incomplete email (below, right) if unable to verify the payee's identity. The team will review the case and reach out with an email from **service@prepaiddigitalsolutions.com** outlining next steps within 5 business days.
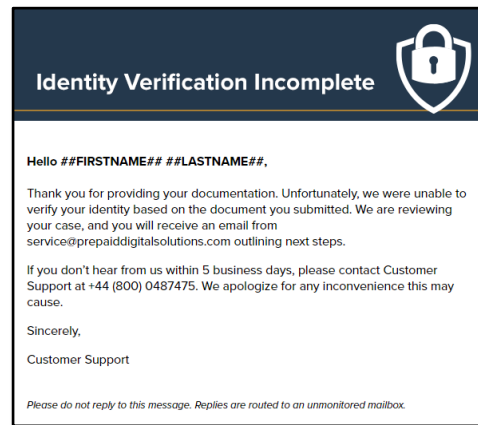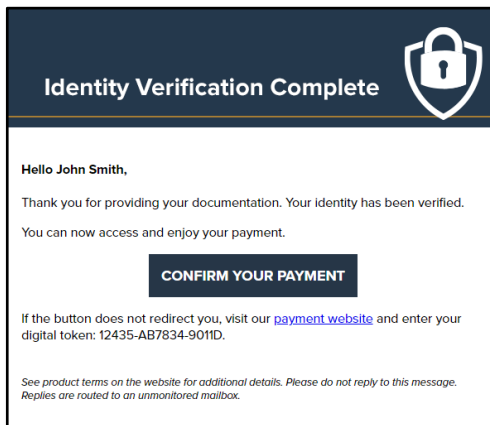
Step 8b: If the payee decides to wait on the site for their results, they will see either the **Success!** or **We're Sorry!** messages.

- On the **Success!** screen, the payee selects OK to continue accessing their payment.
- The **We're Sorry!** screen informs the payee that additional verification steps are required and that an email from **service@prepaiddigitalsolutions.com** will outline next steps.

KYC User Guide

FAQS

Use these frequently asked questions to help answer common Identity Verification questions asked by payees.

Why am I being prompted to verify my identity? I wasn't prompted before.

In accordance with global Anti-Money Laundering (AML) rules and regulations, which are meant to minimize the chance of the payment program being used to commit financial crimes, we are required to complete and validate identity verification.

What are you using to verify my personal information? Is my information properly secured?

After you submit the required information, your identity will be verified by a verification service that will also check various government sources and watchlists. Your information is stored securely per our data protection practices, is only accessed by our in-house team for identity verification and is not shared with any third parties. Please see our **Privacy Notice** for our data protection practices. As long as the information provided is correct and valid, most participants are cleared in real-time and can access their payments immediately.

If I was paid through an employee rewards program, haven't I already had my identity verified since my company who sponsors this program has my information?

Even though your employer validated your identity when you were hired, bank issuance of a card must adhere to banking anti-money laundering (AML) regulations as part of the issuing bank's Know Your Customer (KYC) obligations. As an agent of the bank, we are also required to adhere to the issuing bank's regulations and KYC obligations, just as payees are obligated to adhere to regulations associated with payment access and use. As long as the information provided is correct and valid, most participants are cleared in real-time and can access their payments immediately.

Will I be asked to validate my identity next year or just this one time?

You will be only asked to verify your identity once. However, if regulatory requirements change or if information in your customer profile changes, you may be asked to verify your identity again.

Why was I prompted for a KYC identity verification more than once?

The payment platform tracks cumulative payments for each currency based on the personal email address you use. If you use different email addresses for another payment program or are paid in another currency, you could be required to validate your identity again.

How can I help reduce verification turnaround time?

You will be cleared in real-time provided you correctly entered the required information; your name, primary residential address and date of birth (DOB). In some circumstances — including a recent move — you should enter the address where you are receiving your personal mail. If you do not enter a residential address, you will likely fail a real-time check and our we will request additional documentation.

KYC User Guide

I've uploaded my identity document, why did I receive an email requesting a utility bill to be uploaded?

If, the document you uploaded is unable to be authenticated or if additional information is required, the cardholder will receive an email requesting additional documents (i.e., utility bill) to be uploaded via secure file share (CognitoForms). The utility bill (e.g., gas, electric, internet, phone (landline only); cannot accept mobile) must be recent and within the last 90 days.