Treefort Release Notes

May 26, 2023

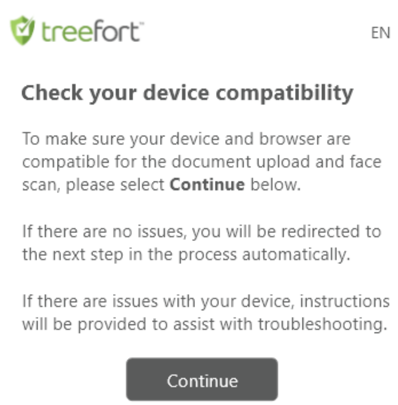
What’s New

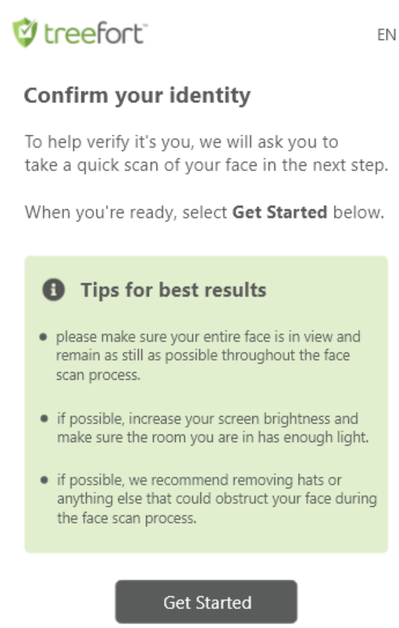
Summary of Major Updates

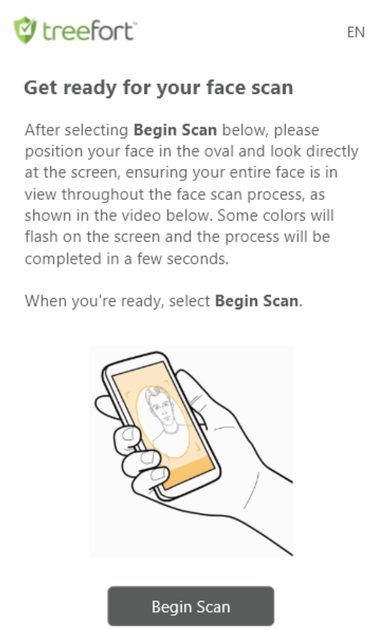
iProov Genuine Presence Assurance ®

We’ve partnered with iProov (https://www.iproov.com), a world leader in Genuine Presence Assurance technology used by banks, governments, and healthcare providers, to provide a quick, secure, and more intuitive way to verify the identity of your clients than ever before.

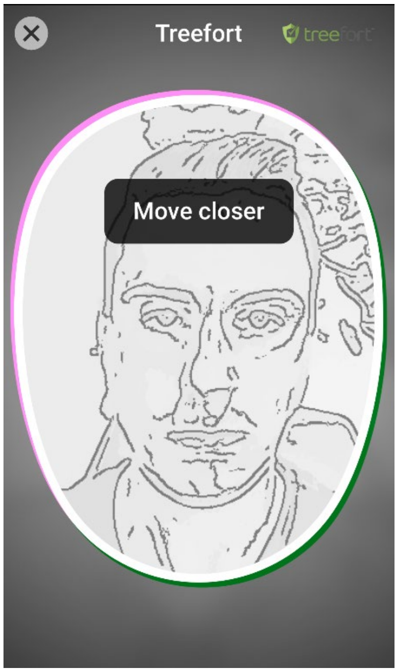
During the ID verification process, clients will continue to upload a government-issued photo ID document and will then be directed to complete a facial verification using iProov’s Genuine Presence Assurance technology. Clients will be prepared for the facial verification by checking their device and browser compatibility and reviewing general best-practices for a successful facial verification, as shown below.

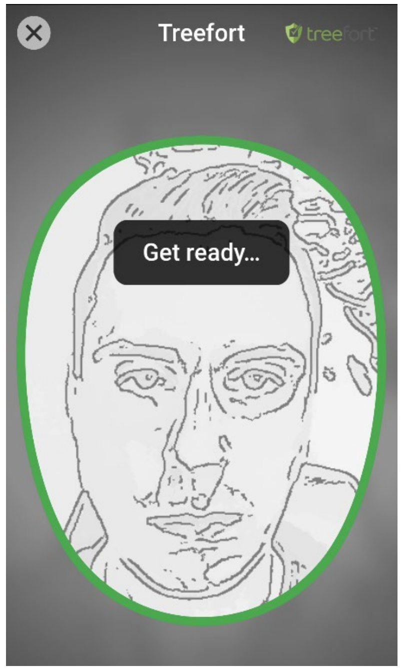






Using iProov’s **passive** user experience, clients will no longer be required to follow on-screen prompts instructing them to move their face or mobile device throughout the facial verification. Instead, clients will now position their face within an oval and remain as still as possible. Once in correct position, the facial verification will begin automatically and will only take a few seconds, as shown below.





Should the client experience an issue preventing them from completing the facial verification (e.g., if the room was too bright or dark, if the client's face was not aligned properly, had their eyes closed, was wearing sunglasses, etc.), on-screen feedback will be provided to assist with subsequent attempts.

After completing the facial verification, iProov will analyze the scan across 2 fundamental areas:

- **Anti-Spoofing:** ensuring that the individual passed the Genuine Presence Assurance check, meaning the individual was able to prove that they were a real person (not a photograph or recording, not wearing a mask, not a deepfake, etc.) and were present during the facial verification.

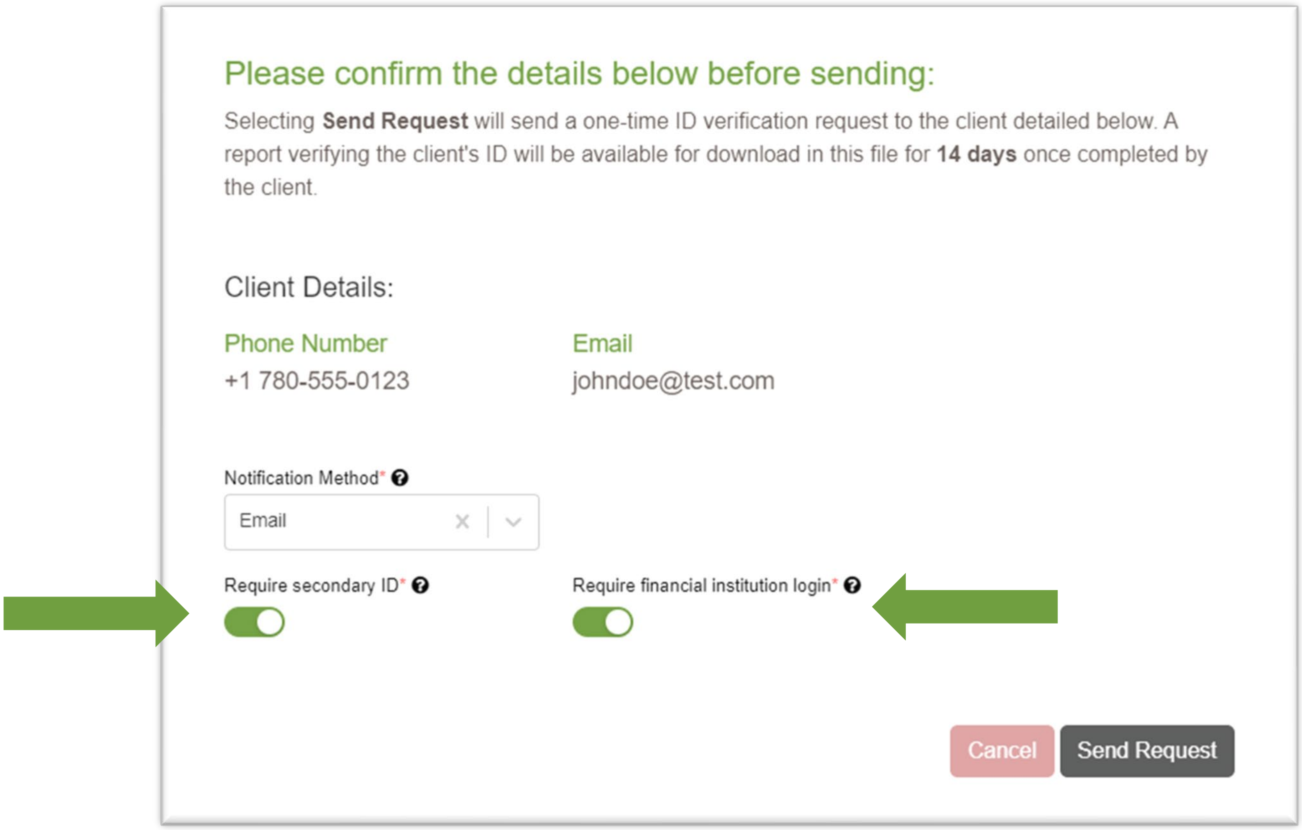
- **Face Match:** ensuring that the photo on the individual's government-issued photo ID matched the face of the individual presenting the ID.

If the analysis flagged any issues, the results will be provided on the Treefort report for review.

Toggle ID Verification Settings

You can now choose if you will require a client to complete the banking login or upload a secondary piece of ID when sending an ID verification request to a client. Previously, these settings were configured as a global setting for your organization and applied to all ID verifications sent on behalf of your organization.

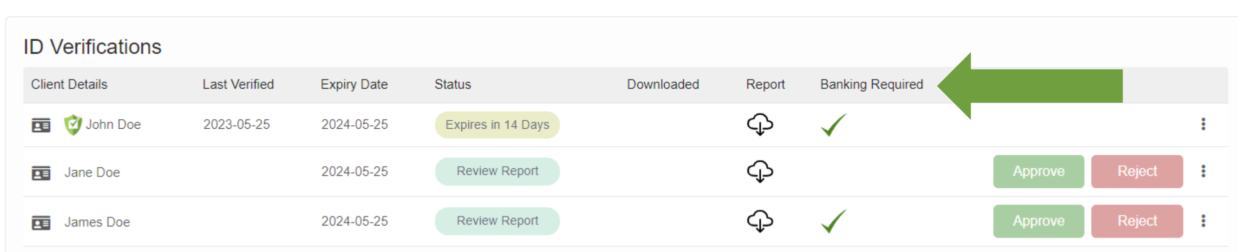
When sending an ID verification request to a client, you will have 2 additional settings to toggle – **Require secondary ID** and **Require financial institution login**, as shown below. **Note:** the selections will default to your organization's settings but can be toggled at the time of sending an ID verification request.



When **Require secondary ID** is enabled, the client will be asked to upload 2 pieces of ID from an approved list during the ID verification process. When this setting is disabled, the client will only be required to upload 1 piece of government-issued photo ID.

When **Require financial institution login** is enabled, the client will be asked to select a financial institution where they hold an online account and will be asked to log into this account through a secure third-party connection during the ID verification process. This will be used to determine if the client has an account with a Canadian financial institution that matches the information used in the ID verification process, and additional risk indicators will be available on the Treefort report returned. Without this enabled, the client will not be asked to log into an account with a Canadian financial institution during the ID verification process.

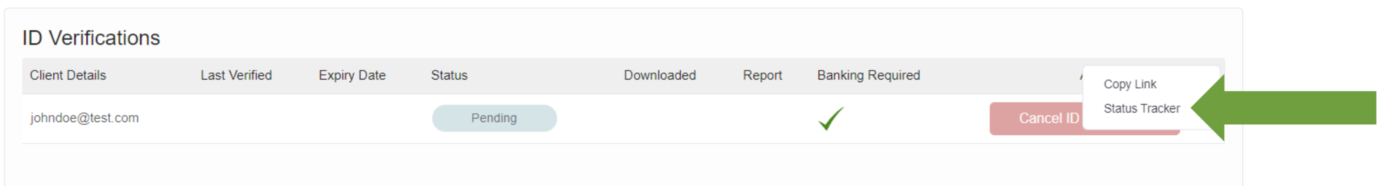
Note: all ID verifications with the banking login required will now be clearly indicated within a file with a checkmark in the **Banking Required** column, as shown below.

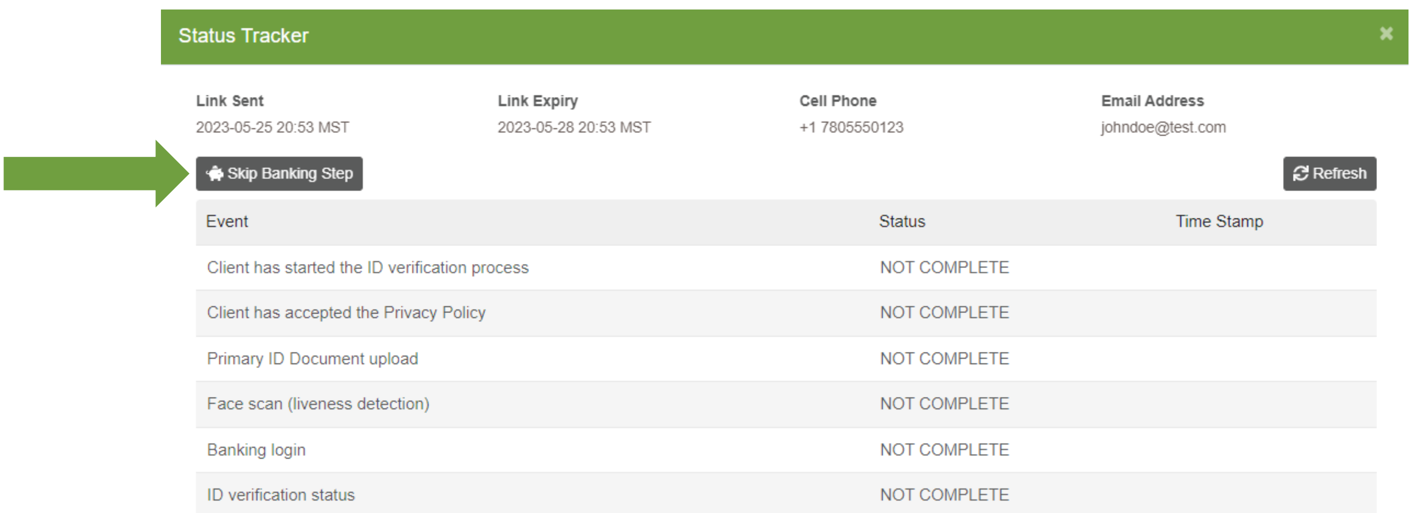


Skip Banking Login

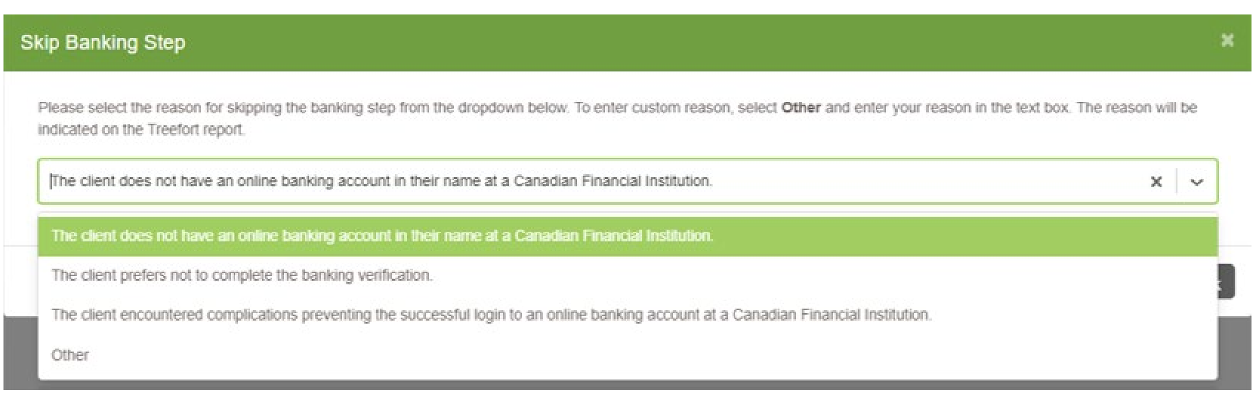
Although you can now toggle the banking login requirement when sending an ID verification request to a client (see the **Toggle ID Verification Settings** section of this document), there may be reasons why a client cannot complete the banking login that are not known prior to initiating the ID verification (e.g., the client does not have online banking). When this happens, you can now skip the banking login requirement while an ID verification is in progress.

To skip the banking login while the ID verification is in progress, select the **Status Tracker** option from a Pending ID verification, then select **Skip Banking Step** from the Status Tracker popup, as shown below.

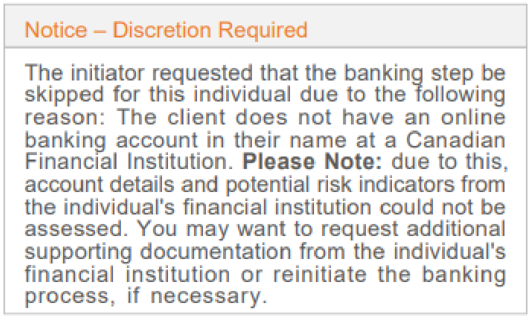




You will then be required to select the reason for skipping the banking login from a dropdown of common reasons, or alternatively, you can select **Other** and enter a custom reason. This reason will be available on the Treefort report for review.

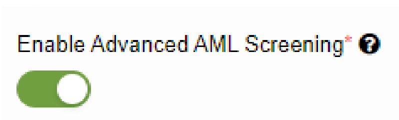


When the banking login is skipped, the client will **not** be prompted to log into their online bank account during the ID verification process, and the Treefort report will be returned without banking information. A **Notice – Discretion Required** risk that includes the reason why the banking login was skipped will be available for review on the Treefort report, as in the example shown below.



Toggle Anti-Money Laundering (AML) Assessment

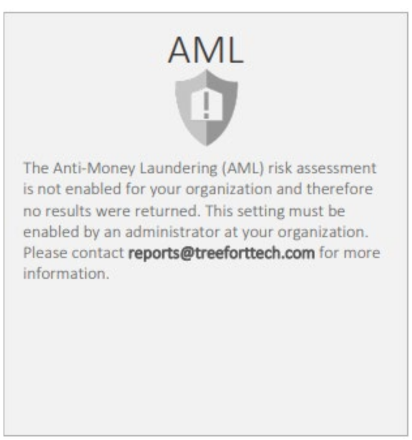
The Anti-Money Laundering (AML) Assessment can now be enabled or disabled from your organization's settings. To adjust this setting, an Administrator at your organization can navigate to **Settings**, where a new toggle for **Enable Advanced AML Screening** will be available, as shown below.



Note: this setting is configured as a global setting for your organization and will be applied to all ID verifications sent on behalf of your organization.

When enabled, the client's information will be screened against a real-time database of Global Watch Lists, Sanction Lists, Fitness & Probity Lists, and PEP (Politically Exposed Persons) Lists during the ID verification process. All possible matches will be available for review in the Treefort report.

When disabled, the AML section of the Treefort report will indicate that the AML setting was not enabled for your organization, as shown below.



Credit File Risk Code Improvements

Any risk codes returned that are associated with a client's credit file will be greatly improved with more detailed information provided directly in the Treefort report. When there is an issue with a client's credit file, risk codes in the Treefort report will now indicate specific reason(s) why the credit file is being flagged (e.g., first name mismatch, last name mismatch, date of birth mismatch, etc.) and will provide the comparison of the information at the credit file and that on the client's ID document. See below for examples comparing previous credit file risk codes and updated credit file risk codes.

PREVIOUS RISK CODE	**UPDATED RISK CODE**
High Risk The date of birth on the individual's credit file did not match the date of birth that was on the individual's government-issued photo ID.	High Risk The date of birth on the individual's credit file did not match the date of birth that was on the individual's government-issued photo ID. **1996-02-05** vs **1992-03-07**.
Medium Risk The individual's credit file has less than 3 years of activity.	Notice – Discretion Required The individual's credit file has less than 3 years of activity. Date credit file created: **2021-03-09**. Please use your discretion to determine if it unusual that the individual does not have 3 years of activity before proceeding (i.e., the individual is not a recent immigrant, does not appear to be too young to have sufficient credit history, etc.).
High Risk A credit file could not be found that matched the name, address, and date of birth on the government-issued photo ID presented by the individual or reported directly by the individual.	High Risk The name on the individual's credit file did not match the name that was on the individual's government-issued photo ID. **Justin Trombley** vs **JOHN DOE**.

Risk Classification Update

When reviewing a Treefort report, there will now be only 2 primary risk classifications – **High Risk** and **Notice – Discretion Required**, as shown in the examples below. The **Notice – Discretion Required** risk classification has replaced the previous classifications of **Low Risk** and **Medium Risk**.

Notice – Discretion Required	High Risk
The individual's credit file has less than 3 years of activity. Date credit file created: **2021-03-09**. Please use your discretion to determine if it unusual that the individual does not have 3 years of activity before proceeding (i.e., the individual is not a recent immigrant, does not appear to be too young to have sufficient credit history, etc.).	The individual failed the genuine presence assurance check, meaning the individual failed to prove that they were a real person and were present during the ID verification process. It is possible that the individual may have been holding a photograph, wearing a mask or other disguise, or using an automated program in an attempt to manipulate the system.

The overall Treefort report conclusions will remain the same: when a **High Risk** is present on a report, the Fraud section of the report will fail, indicating that there was at least one High Risk indicator of potential fraud and additional due diligence is recommended.

All **Notice – Discretion Required** risks should be reviewed, using your discretion and review of the Treefort report in its entirety to determine if you will continue to interact with the client.

Need assistance or have questions? Please contact **support@treeforttech.com** or your Treefort representative and we will get back to you right away!