

This update is the third in a series of communications to market firms regarding the planned shutdown of the old platform (PPL v3). To re-cap, these dates are as follows:

- **1st October 2023:** the option to initiate new placements on the old platform (PPL v3) will be disabled.
COMPLETE
- **15th December 2023:** User access will be disabled, and no further activity will be possible on v3, with the exception of Super Users (for the purposes of accessing MI extracts).
- **31st December 2023:** user access to PPL v3 will be removed.
- Subsequently the platform will be decommissioned, and all data held will be deleted.

The purpose of this update is to provide detail on the process, and associated timelines for market firms being sent and confirming the accuracy of their Audit Trail(s) in readiness for the decommissioning of the platform.

The information contained in this update is as follows:

- **What is happening next.**
- **What is included in the Audit Trail file.**
- **How will PPL be distributing your Audit Trail(s).**
- **How do I access my Audit Trail(s) once I have received my secure USB device.**
- **How will I be able to check the accuracy of my v3 Audit Trail(s).**
 - MI Extracts.
 - Continued super access to v3.
- **What do market firms need to supply PPL to receive their Audit Trail(s).**
- **Actions for market firms.**
- **Frequently Asked Questions**
- **Support & feedback**

1. What is happening next.

After close of business on 15th December 2023, PPL will turn off the 'endorsement' functionality on PPL v3 and restrict platform access to Super Users only (Super Users will retain access for the purposes of accessing MI extracts). This will place the V3 platform in 'read only' mode, after which Ebix will start the creation and extraction of the market's Audit Trails. The intent is for all Audit Trails to have been produced by no later than 31st December 2023. This will ensure distribution of the Audit Trails by PPL can commence from 2nd January 2024, with all market firms being in receipt of their Audit Trail(s) by 12th January 2024.

All market firms will receive their complete Audit Trail(s) via post/courier on highly secure encrypted USB devices (FIPS 140-2 level 3), with the associated PIN and passwords being made available separately to a designated person(s) via a specially created secure web application.

Market firms will be asked to review their Audit Trail(s) by 26th January 2024 for completeness and correctness as PPL will not be able to resolve issues with the Audit Trail(s) beyond this date.

2. What is included in the Audit Trail file.

The single extract Audit Trail will be extracted by Organisation, then by programme, with data starting from day 1 of the PPL v3 platform in order to provide a complete history. Included with the complete set of Audit Trails will be a meta data file. The metadata file will be created at Organisation level for each Audit Trail extract to enable better search capability post download.

NB. If you have more than one organisation set up on the old platform, you will receive an Audit Trail for each organisation.

The extract content will be in the same structure that is available in the old platform via the Messages and Documents screen, e.g., a folder containing a number of files, including the Audit Trail.

For more information on the structure, content, and metadata file, please refer to our July decommissioning update available on the PPL website.

3. How will PPL be distributing your Audit Trail(s).

The Audit Trail(s) will be distributed to market participants on FIPS 140-2 level 3 devices via the Royal Mail Special Delivery or a courier. Each device will be stored in a tamper evident bag and will have a unique serial number printed on the outside.

The level of inherent security associated with FIPS 140-2 level 3 devices means that, if intercepted, they are useless without a PIN and password. This is why the device, PIN and password are all delivered separately.

4. How do I access my Audit Trail(s) once I have received my secure USB device.

The authorised person(s) will need to access a secure web application to retrieve the PIN & password to access the device.

Once PPL has been informed who the authorised person(s) is, they will be contacted directly with instructions on next steps. The reason the instructions are not included within this update is for security purposes.

5. How will I be able to check the accuracy of my v3 Audit Trail(s).

Once the platform is switched into read-only mode, market firms will have three methods for confirming the completeness of their data: -

- 1. MI Extracts.**
- 2. Continued Super User access to v3.**
- 3. Their own company records.**

We will explore points 1 and 2 further in the following sections.

MI Extracts

The PPL v3 platform allows market firms to run a detailed extract to provide a list of firm orders at contract level by organisation hierarchy, contract status and class of business. These can be requested via the old platform, either at risk or transaction level by Super Users until 26th January 2024.

The maximum period for an extract is 367 days, so it is recommended that you download and store each year separately.

It is suggested that you do a compare of the unique records identified in your firm order extract, and the metadata file provided with the Single Audit Trail for each Organisation. This will help you to quickly identify that you have received all your records.

Continued Super User access to v3.

Super Users will have continued access to the v3 platform to either request v3 MI extracts or to view/download messages and documents on a risk-by-risk basis.

On receipt of your single Audit Trail(s), a Super User can spot check placement data on the old platform to ensure it matches.

6. What do market firms need to supply PPL to receive their Audit Trail(s).

- The Organisations for which they require a complete Audit Trail.
- The address that each device is to be shipped to.
- The authorised person(s) to receive the device, PIN, and password.

NB. Please detail each authorised person, should you choose different recipients for each of the above to have segregation of duty.

- The email address and mobile phone number for the authorised person(s).

These details should be sent to audit@placingplatformlimited.com.

7. Actions for market firms.

- a) Determine if your firm wants to obtain copies of your Audit Trail(s), MI Extracts, or both from PPL v3.
- b) Designate an individual(s) to whom the device, PIN and password should be sent.
- c) Inform PPL the names of the designated individual(s) and associated information.

8. Frequently Asked Questions

Q. What is a FIPS 140-2 Level 3 device?

(Federal Information Processing Standard) FIPS 140-2 Level 3 certified devices are designed to prevent physical tampering with tamper-evident seals, intrusion sensors, and self-destruct mechanisms. These devices meet the requirements of Level 3 of the FIPS 140-2 standard.

Q. How do I know FIPS 140-2 Level 3 devices are secure?

They undergo rigorous testing and certification to meet the highest security standards. With Level 3 certification, market firms can rest assured that sensitive information and cryptographic keys are well-protected against physical attacks.

Q. Are PPL sure it safe to send market data on secure devices via Royal Mail/couriers?

Yes. The device on its own is useless without both the PIN and password. The device will destroy all data if the PIN is entered incorrectly 10 times. It is also resistant against physical tampering.

Q. Why do I need a PIN and a password?

The PIN is security for the device, and password is security for data, which is encrypted.

Q. Does the person receiving the secure device, PIN and/or password have to be an existing Super User for that company team, or could it be someone from our internal IT department?

No. We recognise that the data might need to be sent to an IT department, rather than Super Users to upload the data to your infrastructure.

Q. Our USB drives are disabled, is there any other way to get the data?

It is PPL's assumption that the device will be sent to a market firm's IT department for upload onto internal infrastructure. However, if this is not the case, the recipient of the device will need to speak to their internal IT department. If your IT department would like to speak with PPL, please contact audit@placingplatformlimited.com.

Q. How do I know the size of the file I am going to receive?

If you want to find out in advance the size of your Audit Trail file, you can email audit@placingplatformlimited.com and we can provide you with an estimate.

Q. What do we do if the secure device doesn't arrive?

Please contact audit@placingplatformlimited.com to request a replacement.

Q. What if the Audit Trail files on the secure USB device cannot be read?

Please contact audit@placingplatformlimited.com to request a replacement.

Q. What is the make and model of the device we will be sent?

PPL are using iStorage DatAshur Pro2. File sizes below 64GB will be a USB flash drive and above 128Gb, an HDD/SSD.

Q. Do we need to return the secure USB device to PPL?

You do not need to return the device.

Support & Feedback

If you have any questions or queries relating to this document, please contact audit@placingplatformlimited.com.

For all other queries, please contact pplenquiries@placingplatformlimited.com.