



PASA Dashboards Working Group

Resolving Possible Matches – FAQ Approach

Importance of the end-to-end user journey

October
2026

Produced in partnership with:



PASA Experts for Dashboards

PASA 

Acknowledgements

PASA is grateful to the members of the PASA Dashboards Working Group (PDWG) who authored the Guidance and their employers:

Kim Gubler (Board Sponsor)	PASA
Maurice Titley (Chair)	Lumera
David Brooks	Broadstone
Geraldine Brassett	WTW
Kelsey Marriner	XPS Group
Richard Smith	Independent

With thanks to the Money and Pensions Service (MaPS) for its input and contribution to the development of this Guidance.

PASA Dashboards Toolkit
Resolving Possible Matches – FAQ Approach

Section	Content	Page
1	Introduction	1
2	A Principles Based Approach	1
3	Frequently Asked Questions	4
4	Conclusion	10
5	Appendix 1	11

1. Introduction

Possible Matches are a deliberate feature of the dashboards ecosystem, intended to reconnect users with pensions where data is incomplete or inconsistent. However, they introduce significant complexity and risk which must be actively managed. This creates a three-way design tension between:

1. minimising user friction, i.e. additional steps or barriers which result in the user being put off or disengaging with the possible match process
2. maintaining robust identity and fraud controls
3. ensuring operational scalability at volume

Resolving Possible Match (RPM) processes need to balance all three.

A user is prompted to contact an organisation they may not recognise, while the provider is being asked to establish whether the individual is the member associated with the pension record based on partial or inconsistent data. This leads to an inherent tension between minimising friction, in order to support engagement, and maintaining robust controls to prevent fraud and misidentification. But this also creates a great opportunity to improve data in the lead up to and following the launch of the MoneyHelper Pensions Dashboard (MHPD).

This is the first version of the toolkit. It will be reviewed and updated as testing and operational experience develop, ahead of and following public availability of pensions dashboards.

2. A Principles-Based Approach

RPM represents a new and evolving area of pensions administration. As such, this toolkit content is intended to reflect emerging good practice. Providers may arrive at different operational solutions depending on their data, systems and service models, and some variation in delivery is expected.

However, as an outward-facing process, RPM should deliver a consistent and coherent experience for users as they may need to follow the process with several different organisations. The focus should be on supporting the user journey to resolution, balancing engagement, control and operational practicality.

RPM processes should be grounded in a small number of core principles, from which appropriate and proportionate solutions can be developed:

- clear and consistent user journeys
- risk-based design aligned with A-D circumstances (as defined below)
- alignment with the provider's agreed matching policy and PASA's Data Matching Convention (DMC)

Guidance

- operational scalability at volume
- security, trust and mitigation of the risk of misidentification

2.1. User journey clarity

The user journey should be designed to support clear, timely and accessible resolution of Possible Matches. Journeys should be clear and consistent across contact channels, with explicit next steps and messaging designed to reduce confusion where a user doesn't recognise a pension. If journeys aren't well designed, there's a real risk users will disengage, make repeated contact, or lose confidence in dashboards altogether.

Contact routes presented on dashboards are based on provider-supplied data. In practice though, users may choose to engage through alternative channels. Providers should therefore ensure appropriate support is available across multiple channels, recognising reliance on a single contact route may create barriers to engagement, particularly for vulnerable users.

Processes should also ensure enquiries are identified and acted upon promptly. Where a user makes contact within the 30-day period, providers should flag the Possible Match as under investigation so it remains available on the dashboard while enquiries continue.

Care is required in how No Match outcomes are communicated, as these may be unexpected for users and can affect confidence in dashboards, and pensions more broadly.

2.2. Risk-based approach aligned to A-D circumstances

The appropriate balance between friction and control will vary depending on the nature of the Possible Match. Where 'friction' refers to the steps or effort required from the user, and 'control' refers to the strength of identity verification and fraud prevention measures. In practice, providers are seeking to maximise the number of correct matches while minimising the risk of misidentification or fraud.

PASA developed an A-D categorisation to help process designers understand the possible mindset and behaviour of different users. Users are not expected to explicitly self-identify against these categories. Administration teams should be cognisant of these scenarios as these may play a part in how cases are handled. It may be interesting to see how this area develops after the MHPD is launched to the public and what adjustments may be required to providers' RPM processes.

Circumstance	Description	User support considerations
A	Not theirs (user is confident)	Clear explanation and an accessible route to resolve or query the result
B	Not theirs (user unsure)	Reassurance and support to establish whether the pension is theirs
C	Theirs (user confident)	A straightforward route to resolution, with appropriate verification
D	Theirs (user unsure)	Support to investigate unfamiliar pension details, with appropriate verification

These categories describe the user's circumstances and can help providers tailor communication and support. They don't establish identity or entitlement. Verification requirements should reflect the evidence available and the assessed risk in each case, rather than the user's confidence that the pension is or isn't theirs.

2.3. Consistency with provider's matching policy and the DMC Guidance

Possible Match processes can't be designed in isolation. They need to align with the matching policy, the criteria generating Possible Matches, and the DMC principle responses should be sufficiently focused to avoid excessive false positives. While there should be an alignment with existing verification processes a key distinction is, at the Possible Match stage, the individual may not yet be confirmed as the member. Providers should therefore ensure any verification approach is proportionate to this uncertainty and doesn't assume an established customer relationship.

2.4. Operational scalability

At scale, Possible Matches may generate significant contact volumes and, depending on matching criteria and data quality, potentially a high proportion of 'No Match' outcomes. Processes therefore need to be designed so they're operationally efficient and can be monitored and refined over time using outcomes data.

Providers should also understand how the Possible Match process operates within the dashboards ecosystem. A Possible Match will cease to be available if the individual doesn't engage within the prescribed period (currently 30 days). Where the individual makes contact and the case is actively being investigated, providers may maintain the relevant Pension Identifier (PEI) in accordance with the dashboards framework while enquiries continue.

Although there's no prescribed regulatory timeframe to resolve a Possible Match, timely identification and progression of cases remains important to support positive user outcomes. SLAs for possible matches should therefore reflect not only overall turnaround times but also the speed of initial review and triage. Processes should ensure cases are identified and progressed as close to the point of receipt as possible.

2.5. Security, trust and misidentification

Because users are being directed to initiate contact, providers need to assume an elevated fraud risk. However, while the risk posed by bad actors shouldn't be underplayed there's a corollary risk of misidentification.

Identity verification should be at least as robust as business-as-usual processes, with additional checks where the evidence or assessed risk warrants them. The user's familiarity with the provider or confidence about the pension shouldn't, on its own, determine the strength of verification.

2.6. A simple framework for assessing Possible Matches

While provider processes will vary, most Possible Match cases can be considered through four key questions:

1. Is this the individual who received the Possible Match on a pensions dashboard?
2. Is this individual the member associated with the scheme record?

3. If so, what data discrepancy prevented a full match?
4. Is sufficient evidence available to update the relevant records?

The remainder of this document explores the practical considerations associated with each of these questions.

3. Frequently Asked Questions



What's a Possible Match and why is it provided?

A Possible Match arises where a provider's matching criteria indicate a potential, but not certain, link between a user and a pension record. It exists to reduce the risk of incorrect matches and inappropriate data disclosure, while still enabling reconnection where data is incomplete and/or imperfect.

Providers should ensure processes managing Possible Matches appropriately reflect the higher degree of uncertainty inherent in these cases.

In designing Possible Match processes, providers may wish to consider:

- Whether identity verification requirements should differ from those used for fully matched members, given the absence of a confirmed relationship
- What constitutes a proportionate level of assurance, balancing fraud risk against the risk of creating barriers to engagement
- The appropriateness of evidential requirements (e.g. whether requesting original documents is necessary or proportionate in these scenarios)
- How to manage cases where data is incomplete or inconsistent, without over-reliance on strict verification thresholds
- Alignment with existing matching and verification policies, while recognising Possible Matches represent a distinct risk profile



What should providers expect a user to do?

The user will typically see a pension flagged as requiring action, be given contact details for the provider, and then decide whether to follow up. In practice, providers should expect some users won't recognise the pension and some won't follow up at all.



How should contact routes be designed?

Providers determine the contact details presented on dashboards, and this choice has a direct impact on both user experience and operational delivery.

Design needs to consider whether enquiries are routed to specialist teams or existing contact centres, how this will affect operational capacity, and what this means for the user experience. Consideration should also be given to channel choice, including whether to offer web, phone, email or a combination. The consistency within organisations is also important where users have multiple possible matches in different schemes but with the same provider.

Providers may also wish to consider the use of a 'landing page' or initial triage step for dashboard-referred users, e.g. users could be prompted to return to the MHPD to provide or refine key identifiers such as National Insurance Number (NINO) or previous names, where these were missing or incomplete in the original find request. This may help resolve some Possible Matches without the need for direct contact.

Providers should document an explicit contact strategy covering:

- routing (specialist RPM team vs existing contact centre)
- channel mix (web, telephone, secure messaging)
- expected volumes and peak demand scenarios
- potential use of A–D circumstances to inform handling approaches and colleague awareness, rather than prescriptive routing
- and alternative paths for complex or vulnerable users

Use of existing contact centres may improve accessibility but risks inconsistent handling and higher repeat contact rates. Use of specialist teams may improve outcomes and fraud control but creates capacity constraints. Providers should explicitly assess this trade-off.



Should providers use case reference numbers?

Where a reference number is provided through the dashboard, users should be encouraged to quote it when contacting the provider. References can help providers locate the relevant Possible Match and handle enquiries efficiently.

Providers should also have a process for handling enquiries where the user cannot supply a reference. A reference number isn't proof of identity, and possession of one shouldn't be treated as evidence that the enquiry is legitimate.



How should identity verification be carried out?

Identity verification should follow existing business-as-usual standards as a minimum but should also reflect the increased level of risk associated with Possible Matches.

Care is needed where the user doesn't recognise the provider, as is often the case in Circumstances A and B, or where sensitive data may be disclosed. This can be compounded where the individual is reluctant to share personal information because they're unsure whether the pension is theirs.

Providers shouldn't rely solely on dashboard interaction, case references, or unverified information when verifying identity.



How should providers assess a Possible Match?

When a user makes contact, providers should locate the possible match, review the criteria triggering the Possible Match, and compare the find request data with the data held on scheme records. Based on this combined with the outcome of the identity verification process, they should determine whether the outcome is a Match Made or a No Match. It's up to the provider to determine the appropriate Identification and Verification process, which will already be in existence. This process should be reviewed to ensure it remains appropriate.

In practice this may not be a trivial task. Providers will need clarity on both the data supplied by the user and the specific risk indicator or matching criteria leading to the Possible Match in order to make an assessment.



What outcomes are possible and how should they be handled?

No Match

Where the outcome is a No Match, which will often correspond to Circumstances A or B, the provider should record the outcome and ensure subsequent repeat matches for the individual user are handled in line with the [MaPS Pensions Dashboards Technical Standards](#), and specifically paragraph 115, which states future Possible Match responses for the same pension record should be suppressed.

The way suppression is implemented may vary depending on the software and Directly Connecting Organisation (DCO), often referred to as an Integrated Service Provider (ISP). However, once a Possible Match has been confirmed as a No Match, a subsequent find request with the same Find Correlation ID must not generate another Possible Match for that pension record. The Find Correlation ID identifies repeat requests relating to the same dashboard user.

In line with the Technical Standards this suppression of Possible Match responses is permanent, irrespective of any changes in the member's data being compared in a future matching process. However, in an unusual situation where

data changes subsequently result in a full match, meaning the No Match conclusion had with hindsight been incorrect, then full match would be registered as usual.

Where a Possible Match is determined to be a No Match, providers should also ensure the PEI is deleted in accordance with the MaPS technical standards.

Providers should also consider the impact on the individual where a Possible Match results in a No Match outcome. In many cases, the user will have engaged in good faith and may be disappointed or confused by the outcome. How this is communicated matters. Poorly handled No Match outcomes risk undermining confidence not just in the provider, but in pensions dashboards and pensions more broadly.

Clear, empathetic messaging and, where appropriate, signposting to next steps (e.g. checking details or contacting other providers) can help maintain trust and support continued engagement.

Providers should also consider whether separate matching suppression processes are needed. This would be to support the identification and management of suspected fraud or impersonation, in line with applicable data protection requirements, and understand the options provided by their DCO in this respect.

Match Made

Where the outcome is a Match Made, typically corresponding to Circumstances C or D, the provider should record the match decision and apply any relevant data updates. Depending on system design, this may result either from an administrator updating the match status directly or from the matching engine recognising the updated data and automatically converting the case to a Match Made. The case should then proceed as a standard member interaction.

In some instances, a match may trigger further internal processes, e.g. manual value calculations which would fall in line with standard deadlines. Where the member is active, providers should take account of the fact they may not hold the authoritative data and consider whether additional validation or employer engagement is required.

No follow up

There will also be cases where no follow-up occurs. These will expire after a period of 30 days, but providers should define their own approach to follow-up and case closure.

Follow up - not completed

There may also be cases where follow-up is initiated but not completed. Providers should define how such cases are managed, including when and how often to chase the user and when the 'under investigation' flag should be removed resulting in the de-registration of the PEI.

Providers should ensure the handling of Possible Match outcomes remains consistent with the [MaPS Pensions Dashboards Technical Standards](#), including the PEI status transition pathways and deletion reasons described in

paragraph 121. Operational processes should be designed around those defined lifecycle states rather than creating additional dashboard-facing states.



How much friction should be built into the process?

Processes should minimise unnecessary steps while maintaining proportionate identity verification and fraud controls. The level of verification should reflect the evidence available and the assessed risk in each case.

The A–D circumstances can help providers tailor explanations, reassurance and support. They shouldn't be used to reduce verification requirements solely because a user is confident the pension is theirs, or to impose stronger checks solely because they're unsure.



What risks should providers actively manage?

Key risks arise across several areas and are closely connected. There's a clear exposure to fraud and impersonation, particularly where open contact channels (such as web forms) can be exploited, reference numbers misused, or individuals sharing personal information with organisations they don't recognise.

There's also a risk of misidentification. Because Possible Matches are based on incomplete or partially matched data, there's a chance of confirming the wrong person, especially at scale or where names and other details are common.

From an operational perspective, high volumes of No Match outcomes arising from Possible Matches can drive contact spikes and repeat enquiries, particularly if journeys are unclear or inconsistent across channels. This can lead to inefficiencies and increase the risk of error. As noted below high volumes of Possible Matches should prompt providers to review their data and/or matching criteria.

There are also user experience risks. If next steps aren't clear, or No Match cases are handled poorly, individuals may lose confidence and disengage from the process.

Providers could be presented with the issue of missing matches (false negatives) where members aren't seeing pensions they expect to see. While the usual Identification and Verification process will be engaged again it's possible the match hasn't happened due to the size of the scheme or member status. However this circumstance is outside the scope of this document.

Finally, digital channels introduce additional risks. Open web forms may be targeted by bots or spam, and without proper controls there's a risk of capturing inaccurate or unverified data. These risks are likely to be amplified at scale, or where matching criteria are not sufficiently targeted.



How should unresolved cases be handled?

Providers should establish clear approaches to how they follow up with users where appropriate, what constitutes a reasonable response window, and when cases should be closed. While the dashboards framework provides a limited period for the individual to engage following the Possible Match notification, providers should ensure cases under active investigation are appropriately flagged so they remain available while enquiries are ongoing.



What should providers monitor?

Monitoring is critical to refining both matching and resolution processes. Providers should track volumes of Possible Matches, the proportion converted to Match Made, confirmed as No Match, or not followed up, and the effectiveness of individual matching criteria. Where equivalent information is already captured for compliance reporting purposes, providers should seek to make use of data to support the ongoing review and improvement of matching and resolution processes.

Trends over time should also be analysed, particularly where they may indicate underlying data and/or resolution process issues. This monitoring supports the continuous improvement of matching policies and operational processes.



How can the number of Possible Matches be reduced?

Providers should look to improve underlying data quality and review their matching criteria where appropriate. They should also consider how to encourage users to provide key identifiers such as NINO or alternate names and ensure messaging within dashboard journeys supports better data input.

The DMC Guidance emphasises the importance of understanding and targeting Possible Matches carefully to avoid unnecessary volume.



What data protection considerations apply?

Providers should ensure all data is processed in line with UK GDPR principles, retention is limited to what's necessary, and data accuracy is maintained and improved over time. Where appropriate, organisations may wish to seek legal advice on retention and usage approaches, particularly in cases where a Possible Match is ultimately determined to be a No Match. From this will follow updates to Data Policies and Privacy Notices, especially included on forms a user needs to complete.



How should providers treat data obtained during resolution?

Where a Possible Match leads to a Match Made, the interaction should be treated as a standard member contact, and any data updates should be applied subject to appropriate verification.

Prior to this point, providers may be dealing with individuals who aren't yet confirmed as members. In these cases, existing non-member or pre-membership processes may be relevant in handling information and evidence obtained during resolution.

The DMC Guidance highlights the opportunity to improve data quality through this process and the importance of distinguishing between verified data and user-provided, unverified data.

Providers should define how information collected during resolution is recorded, including where the individual is subsequently confirmed not to be the member. Case records should clearly distinguish information supplied by the enquirer from verified member data. Information about an individual confirmed not to be the member shouldn't be used to update the member's personal details.

Any retention of information for reporting, suppression or fraud prevention should have a documented purpose, an appropriate lawful basis and a defined retention period. Providers should obtain advice from their data protection or legal advisers where necessary.



Are there additional scenarios providers should consider?

Providers may also need to consider more complex scenarios. Such as multiple Possible Matches being returned for a single user by the same provider, split administration arrangements including AVCs, transitions from Possible Match to Match Made where value data isn't yet held, and cases where users disengage after initial contact.

There are also the scenarios where multiple users become associated with the same pension record (for example, a new Possible Match arising against a record already confirmed as a Match Made for a different user). The options available to handle these scenarios are also set out in the [MaPS Technical Standards](#) paragraph 117.

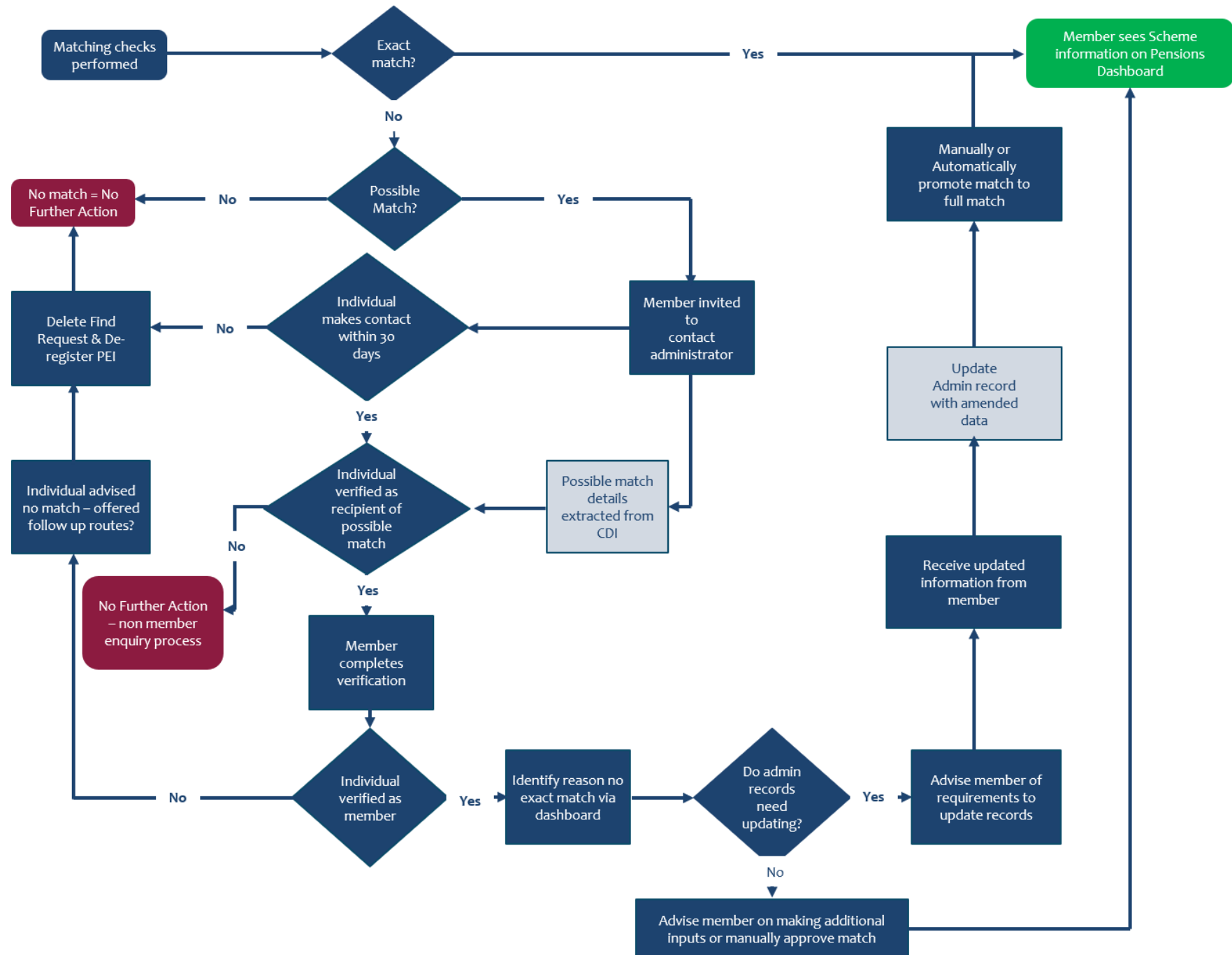
These areas are likely to require further PASA and industry guidance as operational experience develops.

4. Conclusion

Possible Matches are a critical mechanism to support the success of pensions dashboards. Their effectiveness depends as much on the quality of resolution processes as on matching criteria themselves.

Providers should therefore design Resolving Possible Match journeys deliberately, ensure they're aligned to matching policy and risk, and monitor outcomes so approaches can be refined over time.

Appendix 1 - Matching Process Summary



About the Pensions Dashboard Working Group

The PASA Pensions Dashboards Working Group (PDWG) brings together representatives from across the pensions industry, including administrators, legal advisers, consultants and technology providers, alongside representatives from the Pensions Dashboards Programme (PDP) and The Pensions Regulator (TPR).

Established in 2017, the PDWG provides an administration perspective on the development and implementation of pensions dashboards. Its primary focus is to develop practical, good practice Guidance to support trustees, scheme managers, administrators and providers in meeting their dashboards responsibilities.

The PDWG operates through a number of specialist sub-groups, each focusing on specific aspects of pensions dashboards implementation and ongoing operation.

Operational Readiness Sub-Group

This Guidance has been developed by the PDWG's Operational Readiness Sub-Group, which focuses on the practical and operational considerations associated with preparing for and supporting pensions dashboards. Its work aims to help schemes and administrators understand their responsibilities, address operational challenges and develop effective processes to support dashboards delivery.

Meet the Operational Readiness Sub-Group

Kim Gubler
Board Sponsor
PASA Chair

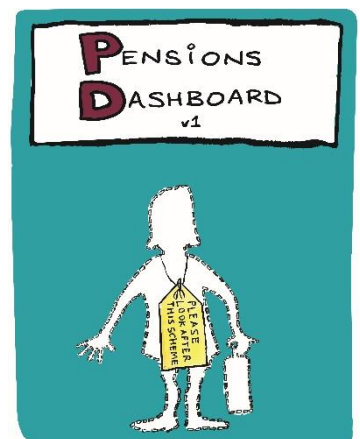
Maurice Titley
WG Chair
Lumera

Operational Readiness Sub-Group Members

Andrew Lowe
Capita
Chris Connelly
Heywood
David Rich
Mortality Manifest

James Bownes
Hymans Robertson
Jayne Wiberg
LGA
Keith Everett
Aptia

Kelsey Marriner
XPS Group
Mark Elliffe
Rothesay
Richard Smith
Independent





Get in touch:

info@pasa-uk.com

www.pasa-uk.com