# PASA Identity Management Working Group

## Protecting Identities During High Risk Events

May 2025

Produced in partnership with:

LexisNexis
RISK SOLUTIONS

Our Experts for
Identity Management

PASA

# Protecting Identities during High-Risk Events

# Acknowledgments

PASA is grateful to the authors of the Guidance and members of the PASA Identity Management Working Group and their employers.

| | |
|---|---|
| Paul Sturgess (Board Sponsor) | **PASA Board Director** |
| Lorraine Salmond (Chair) | **LexisNexis Risk Solutions** |
| Brendon Hogan | **Target** |
| David Cheetham | **Brightwell** |
| Gillian Baker | **Hymans** |
| James Slevin | **Criterion Tec** |
| Rob Hurst | **First Actuarial** |
| Sarah Turner | **XPS** |

## 1. Introduction

Too often overlooked, fraud presents a serious threat to individuals' life savings and pension pots. Pension scams alone cost victims over £26.4 million between 2020 and 2022. With £26.6 billion now held in unclaimed, dormant, or lost pension pots (an increase of £7 billion in just four years) the actual scale of potential losses is likely to be much higher. The way people engage with their pensions introduces a distinct set of risks and challenges for the industry, spanning the entire pension lifecycle.

This Guidance focuses on the interactions likely to pose the most risk, and highlights identity and assurance practices to counter those risks. It isn't statutory and doesn't seek to override guidance issued by regulatory bodies. It's voluntary and seeks to explore the existing and emerging risks within the industry and how those risks may be mitigated. The Guidance is broad in nature, so schemes should ensure their administrators review and align it with their own internal processes and controls.

## 2. Overview of Identity Management

An identity is a combination of 'attributes' (characteristics) belonging to a person. A single attribute isn't usually enough to tell one person apart from another, but a combination of attributes might be.

### What is Identity Management?

Identity management refers to the policies, processes, and technologies used to manage and control the identification, authentication and authorisation of individuals or entities, ensuring the right individuals have the appropriate access to the services and resources they need. The main aim of identity management is to ensure only the real rightful owners are granted access.

### What is Identity Assurance?

Identity assurance refers to the confidence level or degree of certainty an individual's claimed identity is accurate and has been verified to a certain standard. It involves assessing and managing the risk associated with the identification process, ensuring the individual is who they say they are, before granting access to services or information.

Key components of identity assurance include:

- **Identity Proofing**: The process of collecting, verifying, and validating information about an individual to establish their identity. This can involve checking government-issued documents, biometric data, or other trusted sources
- **Authentication:** After the initial identity proofing, ongoing identity assurance may involve the repeated use of authentication mechanisms (e.g. passwords and biometrics) to ensure the individual making contact or accessing a pensions portal or similar system is the same person whose identity was originally verified
- **Assurance Levels:** Identity assurance typically operates at different levels of confidence or assurance, which reflect the rigor of the identity proofing and authentication processes

## What is Identity Verification?

Identity verification is the process of confirming an individual or entity is who they claim to be. This is typically achieved by comparing the provided identity information (e.g. name, date of birth, address, or other personal details) against authoritative sources or using various methods to verify the authenticity of the individual's credentials.

Key aspects of identity verification include:

- **Document Verification:** Checking the validity of government-issued IDs, passports, driving licenses, or other official documents
- **Biometric Verification:** Using physical characteristics such as fingerprints, facial recognition, or voice patterns to confirm identity
- **Knowledge-Based Authentication:** Asking specific questions only the genuine individual would be able to answer
- **Database Checks:** Cross-referencing the provided information with trusted databases, such as credit bureaus, government records, or other reliable sources

## What is Identity Authentication?

Identity authentication is the process of verifying an individual attempting to access a system or service is the person they claim to be. Unlike identity verification, which is typically focused on confirming someone's identity at the outset of a process (e.g. when registering for a portal), identity authentication is about authorising ongoing access

Key aspects of identity authentication include:

- **Password Authentication:** The use of a password or PIN only the individual knows
- **Biometric Authentication:** Utilising unique physical traits like fingerprints, facial recognition, or iris scans to confirm identity
- **Multi-Factor Authentication:** Requiring more than one method of authentication, such as a combination of a password and a one-time code sent to a mobile device
- **Token-Based Authentication:** Using a physical device (like a security token or smart card) or a software token (like a mobile app) which generates or contains a code to login

## 3. Stage of the Pension Lifecycle – Member Data Changes

The best protection available to schemes is to ensure administrators maintain accurate, up-to-date data information for their members, enabling stronger verification and authentication controls, improving member experience, and mitigating the risk of fraud.

One key focus area is data which can be used to determine an individual scheme member's identity. Incremental data changes can seem insignificant at the time, but if combined with insufficient authentication processes, schemes could begin to pave the way for fraudsters.

### 3.1. Identity Risk Considerations

**Online account takeover risk:**

Online account takeover is where a fraudster gains unauthorised access to a victim's online account, such as a bank account, email, or social media profile. The attacker typically uses stolen credentials (username and password) obtained through methods like phishing, data breaches, or social engineering to take control of the account. Once the attacker has access, they can carry out various fraudulent activities, such as transferring funds, making unauthorised purchases, stealing personal information, or using the account to perpetrate further scams, like sending phishing emails to contacts.

In the context of pension schemes, data changes initiated by a ‘claimed’ member pose fundamental risks to both administrators and scheme members. For example, a fraudster adding or removing an authorised signatory.

Small changes overtime, if unevidenced and unmonitored, can lead to big consequences by aiding an impersonator or bad actor.

### Original or copy paper-based requirements:

Sending documents by post increases the risk of exposing personal identity information. It can also discourage members from updating their details, leading to inaccuracies and possible address tracing challenges in future.

### Gone aways:

'Gone aways' occur when individuals moved from their registered address without informing their scheme's administrator. This creates a significant vulnerability, as fraudsters may intercept mail or impersonate the member to gain access to their sensitive pension information. This may result in various forms of fraud, from identity theft to accessing a member's pensions savings. Because these members are no longer receiving correspondence, they can remain unaware of any fraudulent activity. This type of fraud highlights the critical importance of keeping contact details up to date.

A member will become flagged as 'gone away' when they move home and forget to notify their scheme of their change of address.

Managing member data changes in pension schemes, particularly for 'gone aways', requires robust processes to mitigate risks. Addressing these 'gone aways' involves critical decisions, such as whether to suspend pension payments or to allow payments to only continue temporarily. These decisions are especially sensitive for overseas members or vulnerable individuals. For example, those in care homes or under power of attorney. Tax implications may also arise after extended suspensions. Regular mortality screening, address screening and address updates are essential to ensure accurate records and compliance with regulatory requirements.

Fraud prevention is another key consideration, especially in scenarios where both address and bank details are changed or when communication comes from unfamiliar sources. Administrators must establish procedures to flag returned mail as a potential risk and implement a layered response. This could include sending recorded delivery contact letters, initiating a trace, or requiring members to verify their identity before updates are processed. Where contact is lost, gathering evidence of previous and current address data or requesting signed witness statements can provide additional verification.

### Social engineering:

Social engineering is a manipulation technique exploiting human psychology to gain unauthorised access to systems, networks, or information. Instead of hacking into systems using technical means, social engineers trick people into breaking normal security procedures. Common tactics include phishing emails, pretexting (creating a fabricated scenario to obtain information), and baiting (offering something enticing to lure victims).

The goal is to deceive individuals into divulging confidential information or performing actions to compromise security. Social engineering is effective because it leverages trust, fear, urgency, or the desire to be helpful – which are all natural human responses. For example, data changes could be initiated by a genuine but vulnerable member who is being pressured or manipulated to make inappropriate data changes, such as beneficiary or bank account details.

Balancing vulnerability and the risks of social engineering can be challenging for schemes to manage. They need administrators and systems to be sympathetic to various situations members can find themselves in while upholding processes and minimum requirements.

## 3.2. Mitigating Risks During Member Data Changes

**Account takeover:**

Administrators should establish robust minimum standards to limit unauthorised or non-evidenced data changes, and ensure clear processes are in place for handling escalated cases. Administrators should remain alert to signs of vulnerability and take steps to understand the underlying reasons for each request.

Transfers have historically been where pension scams were concentrated. However, administrators should be aware of the growing trend of 'authorised fraud' where individuals are manipulated into doing something which leads to a bad actor's financial gain. For this type of fraud and identity risk it's difficult to spot whether the administrator is dealing with the genuine member. To counter this, it's vital administrators invest in training to help their people identify and support vulnerable individuals. For example, can they clearly articulate what they need to in a confident manner, are there any indications of urgency from the member, is someone acting on their behalf?

The administrator can also record vulnerability flags or markers to member records to allow better handling of the risks associated with this type of fraud while also ensuring there is a process for ongoing monitoring.

When data changes are requested, administrators should authenticate the member making the change. Where there isn't the means to authenticate the member, the administrator should look for evidence of the change and use authoritative sources to confirm it. For example, when people move home, individuals often update their financial accounts first – sometimes this is all that's updated. Data suggests less than half of UK members notify their administrator of a house move. As such, Credit Bureau data is often the first reflection of change.

Administrators should pay particular attention to changes to contact details, particularly email addresses and phone numbers. Any such change should be confirmed through an alternative communication channel. For example, verifying a new email via phone number or vice vera. Where this isn't possible, such as where an old number is no longer active, administrators should layer several authentication checks to ensure the request is coming from the member and acknowledge the change by writing to the home address.

To enhance data accuracy and member engagement, administrators should adopt regular tracing, mortality screening, and existence checks, alongside offering secure online portals for updating personal details. As pensions dashboards are introduced, they promise to streamline data updates and improve member interaction. Each scheme's administrator should tailor its processes based on its member demographics. Active schemes can leverage employer data, while closed schemes should invest in regular tracing exercises to maintain accurate records and reduce risks.

**Original paper-based requirements:**

Administrators can verify name changes by gathering specific evidence, such as official documentation – passport or driving license. If documents are required, administrators should supplement this with further verification to ensure the evidence provided is consistent with what's known of the member's identity.

Enhanced verification could include other forms of identity authentication, such as document verification alongside biometric checking. In certain circumstances this can provide a superior customer experience, e.g. if a member is living overseas. These approaches allow members to verify their identity without the risk of posting important identity documentation.

### 3.3. Emerging Identity Risk Considerations

**Fraudulent Identities, deep fakes and artificial intelligence (AI) generated documents:**

Documentary evidence is often heavily relied upon, especially as a second-line defence where standard identity verification hasn't, or can't, be met. With the acceleration of AI in recent years and its increasing accessibility, the use of AI to create and/or manipulate documentary evidence is on the rise.

Biometrics are used to remotely verify the identity of individuals by comparing the image held on an identity document to one provided by the member. Schemes should be aware when employing a biometric solution or using documentary evidence. This is a risk and you should ensure any administrator is operating to appropriate standards.

## 4. Stage of the Pension Lifecycle - Transferring pension scheme benefits:

A transfer event represents one of the highest risk points in the pension lifecycle, often involving the movement of a member's entire pensions savings. If this transfer is stolen or misdirected to an incorrect account, it may go undetected until the member comes to retire, often years later. By then, the loss could financially devastating, leaving them with little or no opportunity to recover. The consequences could be life changing, potentially forcing them to delay their retirement or accept a materially reduced retirement income.

Transfers can also occur during particularly stressful times such as divorce, moving abroad or moving jobs. Verifying and authenticating members, schemes and advisors remotely calls for the most secure and sensitive identity practices. Additional checks are also advised depending on the administrator's risk-based approach and the risk profile of the other parties involved in the transfer.

Pension transfer identity risks should be considered by both the ceding and the receiving schemes administrators with additional focus if the transfer is coming from, or going to, an overseas scheme.

## 4.1. Identity Risk Considerations - Transfers Out

### Incorrect data:

While certain restrictions apply upon the approach to retirement, a transfer can occur at almost any time for deferred members. Where administrators haven't maintained data accurately during the period of deferment there's an increased risk address and contact details data is no longer accurate.

Schemes must verify the identity of the member before paying the transfer. The transfer event and its associated risk will be increased if incorrect data is held. A proactive approach to data management will reduce this risk and the associated downstream costs.

This risk will likely evolve significantly as members interact with their administrators digitally, the public becomes more engaged and as more information becomes readily available via pensions dashboards. Improving identity management for deferred members will become more of a priority[1].

### Member/other party behaviour:

As part of the transfer due diligence, the administrator must investigate the member's circumstances to assess the transfer against red and amber flags, which is documented comprehensively in PASA's Transfer Guidance. It's important to assess (amongst other things):

- the member's personal circumstances – e.g. to verify if they've not been pressured into making the transfer
- the Independent Financial Advisor's (IFA) situation – e.g. was the member provided any unregulated advice
- the circumstances around how the transfer was initiated – e.g. was the member cold-called or approached? Were social engineering techniques involved?

[1] www.pasa-uk.com/wp-content/uploads/2021/11/PASA-Data-Controls-Guidance-FINAL-1.pdf

**Divorce:**

While scams are deliberate there may be opportunistic fraud opportunities. A good example would be considering the risk of a soon-to-be ex-spouse accessing retirement assets during the divorce process. During divorce, it's vital to ensure the person you're dealing with is the correct individual. Spouses can be unknown to the administrator and therefore carry increased risk.

Even when legal orders such as a pension sharing order are involved in a divorce, it's vital administrators verify the identity of the spouse before making payments. This is to ensure they're dealing with the correct individual and helps mitigate the risks noted above.

**Deceased member:**

Where a member has died, but the administrator hasn't been notified, there's a risk of an individual fraudulently access the deceased's pension benefits, before notification of death is received.

Where a member has a very short life expectancy, extra care is needed in verifying their identity, personal circumstances and the stakeholders involved. The administrator needs to balance the member's vulnerabilities and increased risk of fraud, particularly where there are potential benefits for the member's next of kin. For example, moving funds to a scheme with benefits more tailored for inheritance purposes.

## 4.2. Mitigating Risks During Transfers Out of Scheme *(Applicable to all transfers)*

**Verify the requestor:**

The transferring scheme must verify the member's identity. Administrators need to have dynamic tools and processes to allow them to adjust their verification approach. The process should include the initial identity risk determination alongside what's known about the member. For example, if they've never engaged with their pension before, reliance on authenticators such as one-time passwords isn't possible.

Depending on the individual, their situation, and their previous interactions with the administrator there are several common ways to verify members. The robustness of these checks will depend on several factors and should be considered when choosing verification methods such as:

- How was the information being used to verify the individual collected? Was it collected in a secure manner and safe from manipulation?
- Is the information being used to verify the individual likely to have been exposed to people other than the member? For example, if out-reach letters commonly contain member number and name these shouldn't be relied on alone to verify identity, as there's a risk information has been exposed to others

- How up to date is the scheme's data and can the information being used be relied on? Data decays at different rates therefore asking a member to confirm their contact number collected 12 years ago may not be reliable

Verification approaches should combine a layering of different verification or authentication methods to achieve the most secure identity protection, such as:

- Asking the member to confirm something only they know, this could be a unique scheme identification number, a password, pin or a additional security credentials set up at the time of enrolment or first interaction
- Asking the member to confirm key information, such as their current address, historic addresses, name, date of birth, National Insurance (NI) number and contact details
- Asking the member to confirm something they receive, such as a code sent to contact details known to them. This is called a one-time password
- Document-led Biometric checking

### Authenticate the receiving scheme or entity:

Transfers can proceed when the receiving scheme and, if applicable, the IFA, has been authenticated and relevant transfer guidance has been followed, including assessment of amber or red flags.

Administrators should be aware fake companies can be set up to mirror legitimate companies listed on Companies House. Fake regulatory disclosure details can be provided, e.g. if an IFA were to mimic an FCA-regulated firm. Administrators must conduct thorough due diligence by verifying company details against trusted sources, such as the FCA Register, to confirm the legitimacy of any firms involved in a transfer.

### Overseas scheme transfers:

Overseas scheme transfers pose a much higher risk. For identity risk, the individual may already have left the UK, or left some years ago. If they're still in the UK, the administrator may need to question why they're moving their funds to an overseas scheme. This means data points and processes normally relied on may not be suitable. In these scenarios, additional care is required when authenticating the scheme and the individual, and consideration should be given to an enhanced approach, where available.

### Incorrect data:

Administrators must ensure member data is correct. The transfer event and its associated risk will be increased if incorrect data is held and requires correction during the process. Taking a proactive approach to data management reduces this risk and its associated costs. Refer to the ***3. Member Data Changes*** section of this guide.

**Spouse Identity:**

To verify the identity of an ex-spouse, it's necessary to provide proof of identification. These funds won't be transferred directly to a personal account.

### 4.3. Identity Risk Considerations - Transfers Into a Scheme

Risks can be mitigated when transferring into a UK scheme through application of the same identity verification techniques used for transfers out to UK schemes. However, there are additional risk considerations when transferring from overseas schemes.

**Transfers from overseas:**

It's important to assign appropriate risk when transferring from overseas, and understand the source of funds. In some locations, the tools typically used to assess the legitimacy of the transfer may not be available – making due diligence even more critical.

### 4.4. Emerging Identity Risk Considerations

**Synthetic identities:**

Synthetic identities combine stolen data with other real or invented data, such as false names, dates of birth and addresses. The resulting fake identity is then used to commit acts of fraud. Synthetic identities are dangerous as they combine both real and fake elements. They're often created by fraudsters years before their intended fraud use, over this time the synthetic identity will be used to build an identity footprint. These synthetic identities can look exactly like genuine members with name and address changes.

## 5. Stage of the Pension Lifecycle - Member Retirement

At retirement, there's the risk of large lump sums being diverted to fraudulent individuals. In some respects, this stage of the lifecycle can pose more risk than a transfer due to there being fewer legislative requirements and constraints.

### 5.1. Identity Risk Considerations

**Pension information being sent to wrong or outdated address:**

This can expose details of a pension to unintended audiences

**Impersonation fraud:**

Internal fraud by a work-place employee (such as an administrator) can use privileged access to sensitive information to impersonate the claimed identity or to set up a ghost account.

**Incorrect details provided in error:**

If a member provides incorrect bank details, payment can be made to the wrong beneficiary.

**Family member or financial advisor identity theft:**

Imposters claiming the identity of an authorised party such as a family beneficiary or an authorised financial advisor.

**Overseas members:**

This presents a higher risk due to the reduced ability to contact the member, plus the lack of processes and tools required to confidently verify any overseas documents provided. This leaves the member open to risk of impersonation.

## 5.2. Mitigating Risks at and During Retirement

**Pension information being sent to wrong or outdated address:**

Administrators should limit the details sent in member communications to reduce exposure to data which could later be relied upon for authentication. The content contained in member communications should be noted as part of the scheme processes to ensure authentication processes account for this. For example, if member number, name and postcode are contained in the first contact letters, these points on information shouldn't be relied upon to confirm the member is who they say they are.

Additional approaches to tackle this challenge are those seeking to continuously maintain high-quality accurate data over the member's lifetime. This approach can reduce the risk of data exposure. For example, by ensuring a member isn't being contacted at an address they've since moved away from. This approach can also achieve quicker access to services at a later stage. Another benefit to this approach is the reduction in associated tracing costs.

**Internal identity theft by employer:**

In this scenario there's an array of information relating to the individual available. This means asking the individual to provide information such as their NI number won't provide any assurance. This scenario highlights the importance of an administrator having multiple authentication mechanisms including unique information or ownership only the member would know/could confirm. Administrators should confirm the identity of the member at the point of interaction and the approach will differ based on historic interactions with the member. For example, where a member has already accessed their account online and set-up two-factor authentication (2FA), this provides strong authentication as this wouldn't be information an employer would have available to them.

Where a member hasn't interacted with the scheme and therefore doesn't have the 2FA option available to them, identity verification should be completed. This could include confirmation of identity at the given address, confirmation of historic addresses (though the scheme should be mindful of employment and address overlap), providing identity documents or knowledge-based authentication, which asks the individual an array of questions only they should know the answer to.

### Incorrect details provided in error:

The scheme should confirm the member's ownership of the bank account the pension payment will be made into. There are several bank account verification tools available. Some will confirm the bank account details in relation to the individual and the address associated with the account, these services provide the strongest confidence. However coverage isn't 100% of all accounts and therefore schemes will need additional measures in these cases.

Confirmation of Payee, which enables consumers and businesses to check the name associated against the sort code and account number provided can be used. However, administrators should be aware fraudsters and bad actors can create accounts matched to the name of the intended recipient. If digital confirmations aren't possible bank statements can be relied upon.

### Family member or financial advisor identity theft:

When someone claims to be an authorised person, their identity must be verified. Although the scheme may hold some details about these individuals, it often has limited ability to fully authenticate them. Administrators should take the opportunity to confirm and secure up to date correct contact information, enabling 2FA for authorised parties engaging with the scheme online. Where this isn't available robust identity verification should be employed.

Many administrators will have an appropriate process for enabling power of attorney (PoA) for members. Appropriate due diligence regarding the PoA should be in place. The Office of the Public Guardian maintains records of lasting PoA, enduring PoA and deputyship court orders[2][3].

The administrator should be aware of the possible risk of vulnerability of members and should seek to confirm any requests made by authorised parties with the members themselves, where appropriate.

### Overseas Member:

In these scenarios additional care is required when corresponding with individuals and, where available, consideration should be given to an enhanced approach. For example, specialist forensic services for overseas checks, conducting email address checks, or using a biometric identity check.

[2] https://assets.publishing.service.gov.uk/media/66aa5b44ab418ab05559312b/opg100-find-out-if-registered-attor-large_print.pdf

[3] Office of the Public Guardian (Scotland) (publicguardian-scotland.gov.uk)

### 5.3. Emerging Identity Risk Considerations

**Fraudulent identities and deep fakes:**

Biometrics are used to remotely verify the identity of individuals by comparing the image held on an identity document to a selfie photograph taken by the member. Fraudsters are circumventing these checks by using AI to manipulate and generate documents appearing to be genuine. AI can be employed to mimic the presence of an individual in a live context i.e. being able to replicate a liveness check.

## 6. Stages of the Pension Lifecycle – Member Death

**Member Passes Away:**

The loss of a loved one is a stressful event, and this can result in omissions and errors within the notification process. This stress also makes individuals vulnerable, whether putting their trust in someone they shouldn't or taking incorrect advice.

### 6.1. Identity Risk Considerations

1. **Not informing the scheme of a member's death:**
    1. This could lead to continuing to pay the deceased member resulting in overpayments and potential tax implications.

**Falsely attesting members are still alive:**

Family members, close friends, or the PoA representatives could fraudulently respond on behalf of the deceased member.

**Beneficiary changes or additions:**

There may be tax implications of unauthorised payment being made to someone who isn't the correct beneficiary under scheme rules. e.g. family account paid into/attorney account not in member's name etc.

**Member dying overseas:**

When a member dies while residing overseas, several risks and challenges can arise. Confirming the death of a member abroad can be challenging due to differences in death registration processes and a potential lack of reliable communication or record-keeping in some countries. Verifying necessary documents like death certificates and wills from foreign authorities can be time-consuming and complicated, particularly if the documents need to be translated or authenticated.

### 6.2. Mitigating risks following the death of a member

**Not informing the administrators of the member's death:**

It’s important for administrators to be informed as soon as possible when a member has passed away. The death of a friend or family member is a stressful event and can be worsened by the administration which follows. Several solutions exist to help administrators proactively identify the death of a member as soon as possible. This helps initiate the consequent case processing efficiently and effectively, as well as reducing the likelihood of overpayments.

Administrators should have appropriate mortality screening processes, including a process for scenarios out of scope of standard mortality screening, such as a member living overseas or a member with a PoA in place.

Outside of mortality screening, schemes should have processes which spot and address signals of a potential member death, such as returned post or returned pension payments. A proactive approach will always provide the best solution.

### Falsely attesting members are still alive:

Administrators should review their processes to introduce stronger controls if they currently solely rely on a write-out approach (see mortality screening references above).

In some cases where processes and data provide conflicting information, it may be necessary to employ methods with greater scrutiny, such as biometric checks when contact is made by the member or family member.

### Omitting potential beneficiaries:

During the processing of death benefits, whether spouse benefits or lump sum benefits, administrators need to collate information regarding the beneficiaries. Administrators should identify inconsistencies or apparent omissions when doing so. This may include reviews of expression of wish form/s and copies of the member's will. The legal representative of the member will normally be asked to provide information of this type.

### Beneficiary changes or additions:

Long periods of time can pass between points of contact with a member; therefore, schemes may need to be aware of changes such as divorce and remarriage. Beneficiary checks should include identity verification and living as stated checks.

Schemes should pay attention to the type of request being made by the beneficiary, if schemes have lump-sum options these should be treated as high-risk. In these cases, the beneficiary making the request should prove their identity with tools such as biometric checks.

Beneficiary changes often require marriage certificates and birth certificates. Copies of these documents are often accepted but the administrator should also confirm the identity of the beneficiary to triangulate and verify key elements held on these documents.

## 7. Conclusion

While this Guidance offers a general framework, schemes and administrators should always refer back to their own scheme rules and internal processes.

Fraudsters are constantly evolving, and so must administrators defences. Protect members and their lifetime savings by putting strong, proactive measures in place. Knowing members and confidently recognising them online isn’t just optional, it’s fundamental. Accurate, complete data and rigorous identity verification are the first lines of defence – at onboarding and then at every subsequent touchpoint. Use a layered, resilient approach to defend against identity fraud risks:

- Continuously review data quality – automate data updates to ensure the completeness and currency of members’ name and address data on an enduring basis
- Apply multi-dimensional fraud and identity checks, leveraging extensive data resources, to confidently identify and verify individuals
- Provide members with robust online identity verification services enabling them to prove their identities remotely

## Glossary of Terms

### Authentication Factors:

An authentication factor is a category of credential is intended to verify, sometimes in combination with other factors, an entity involved in some kind of communication or requesting access to some system is who, or what, they're declared to be.

The three categories of authentication factors are generally broken down as:

1. Knowledge factors – a knowledge factor is something you know, such as a username and password
2. Possession factors – a possession factor is something you have, such as a smart card or a security token
3. Inherence factors - an inherence factor is something you are. This includes biometric factors such as a fingerprint, voice or iris pattern[4]

### One Time Password:

A one-time password (OTP) is an automatically generated numeric or alphanumeric string of characters authenticates a user for a single transaction or login session. An OTP is more secure than a static password, especially a user-created password, which can be weak and reused across multiple accounts.[5]

### Synthetic Identity:

Synthetic identity theft is a form of fraud where an identity thief combines stolen information, such as a victim's NI number, with other real or invented information, such as false names, dates of birth, and addresses. The resulting fake identity is then used to commit acts of fraud.

### Two-factor Authentication:

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different *authentication factors* to verify themselves. 2FA is implemented to better protect both a user's credentials and the resources the user can access.[6]

[4] https://www.techtarget.com/searchsecurity/definition/authentication-factor

[5] https://www.techtarget.com/searchsecurity/definition/one-time-password-OTP

[6] https://www.techtarget.com/searchsecurity/definition/two-factor-authentication17

PASA

Get in touch:

info@pasa-uk.com

www.pasa-uk.com

PASA is a Community Interest Company and our full name is Pensions Administration Standards Association CIC.

Company number: 6597097