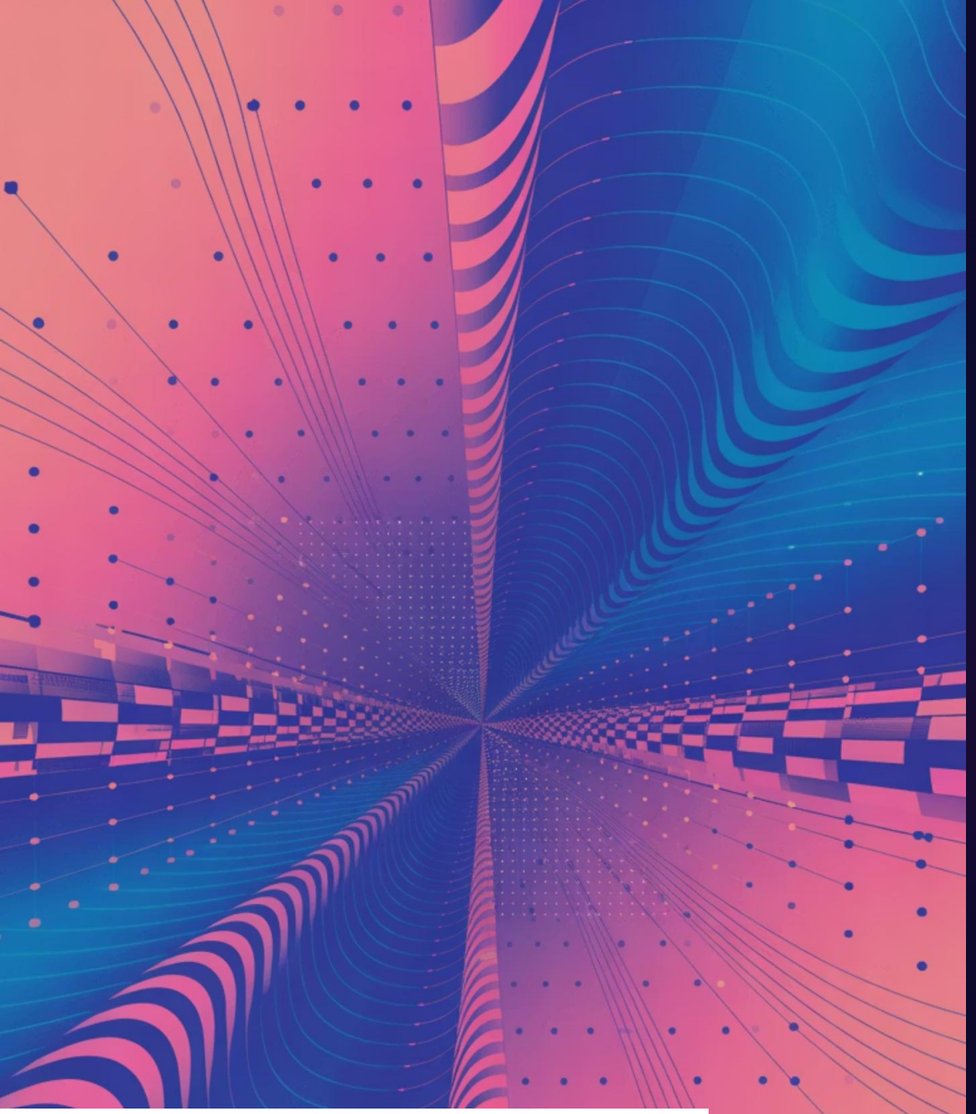


PASA

# Cyber & Fraud Information Sharing Network

## Launch Discussion

Protecting UK pensions through collaborative intelligence sharing

# The Scale of Cybercrime & Fraud

## $23T

### Projected Global Cost

An IMF report predicted cybercrime will cost $23 trillion globally by 2027

## 175%

### Growth Rate

This represents a 175% increase over 2022 levels, showing exponential threat growth

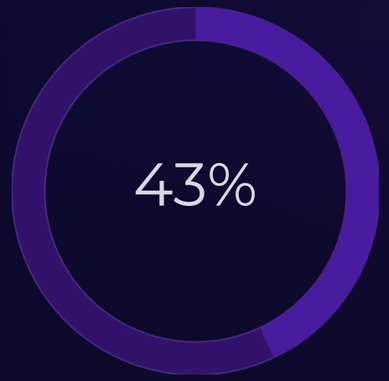
## 75%

### Cloud Intrusions

Cloud security intrusions increased by 75% in 2023 alone as attackers target modern infrastructure

---

## UK-Specific Statistics

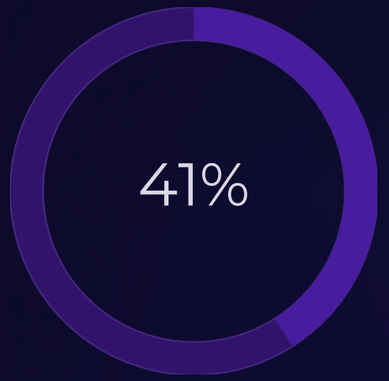



### Businesses Impacted

The UK Government estimates 43% of businesses experienced cyber attacks in the last 12 months


### Charities Affected

Three in ten charities have been impacted, showing the breadth of targets




### Fraud's Share of Crime

Fraud represents 41% of all crime, yet only 14% is reported to authorities

**Reporting of cyber events to organisations' leadership is high, but external reporting remains much lower – creating an information gap this network aims to address.**

# The Unique Impact on Pension Schemes

## Why Pensions Are Different

When M&S and the Co-op suffered cyber attacks, consumers could simply shop elsewhere. The recent Jaguar Land Rover attack saw the government intervene to protect the supply chain – and consumers could wait or purchase alternative vehicles.

**A pension scheme member can't make such choices.** They can't move their administration elsewhere during a cyber or fraud event. They're entirely dependent on their scheme's resilience and recovery capabilities.

## Rich Data Targets

Pension schemes hold extensive member data:

- Individual identification details
- Bank account information
- Employment histories
- Beneficiary data

## Devastating Member Consequences

### Income Payments Suspended

Pensioners unable to receive their regular income payments, impacting their ability to meet essential living costs

### Death Claims Delayed

Beneficiaries unable to access death benefits during already difficult times

### Retirement Lump Sums Frozen

Members unable to access their tax-free cash at the point of retirement

### Investment Switches Halted

Members unable to adjust their investment strategy during market conditions

### Transfer Values Blocked

Members unable to consolidate pensions or move to alternative arrangements

**The consequences extend beyond members: The economic impact on providers could be overwhelming through loss of reputation, regulatory penalties, remediation costs and potential legal action. It's, of course, also a significant regulatory event requiring immediate notification and ongoing reporting.**

# What PASA is Doing

### Building a Network

PASA is establishing a network of pensions professionals to share information on fraud and cyber events, enabling the industry to learn collectively and protect savers, schemes and providers

### Confidential Sharing

The network will confidentially share and discuss anonymised event information, allowing other schemes and providers to learn from incidents and check their own systems for similar risks or vulnerabilities

### Solution Strategies

Sharing will include proven strategies on how issues were managed and rectified, providing practical guidance on incident response and remediation approaches

### Comprehensive Scope

The forum will discuss both cyber security events and wider fraud events, ensuring holistic protection across all threat vectors facing the pensions industry

**This collaborative approach recognises collective intelligence is our strongest defence against evolving threats to pension schemes and member data.**

# Why We're Doing It

## Widespread Industry Impact

We have witnessed extensive publicity of cyber and fraud events across numerous UK industries, demonstrating that no sector is immune to these threats:

- Retail organisations
- Logistics companies
- Manufacturing facilities
- Financial services institutions
- Broadcasting networks
- Even a children's nursery, as reported by the BBC on 2nd October

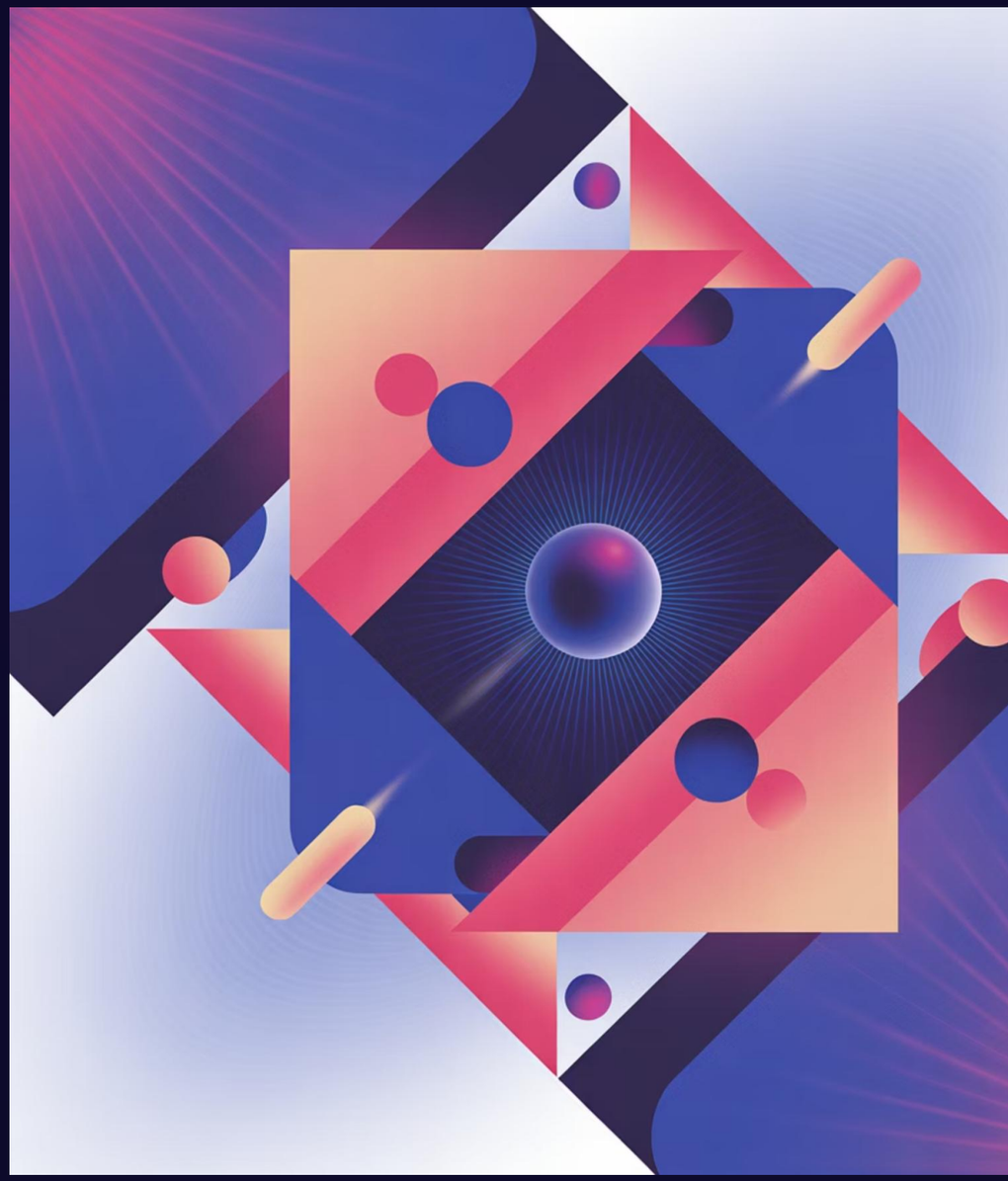
**The perpetrators will consider any industry as potential victims without hesitation, making proactive defence essential.**

## Pensions Already Targeted

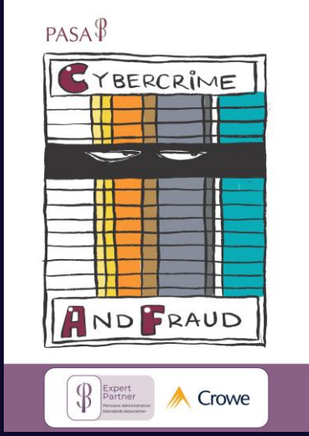
The pensions sector has already been impacted by significant events affecting:

- Third-party administrators managing multiple schemes
- In-house pension scheme operations

**There will almost certainly be more schemes impacted than are in the public domain. Many incidents will have been serious but ultimately unsuccessful – yet these still offer valuable learning opportunities for the wider industry.**



# What the Network Is




## Expert Development

The PASA Cyber & Fraud Information Sharing Network has been developed through the PASA Cyber & Fraud Working Group, comprising representatives from a wide range of PASA members

## Diverse Expertise

The Working Group includes information security specialists, fraud specialists and legal advisers, it’s chaired by PASA's expert partner in fraud and cyber security, Crowe, working alongside the PASA Board

## Anonymous Sharing

Members submit anonymised information about events that have impacted their schemes and organisations, or events they have become aware of more widely across the industry. A standardised approach is followed for all submissions via a proforma.

## Collective Learning

The objective is for the industry to learn collectively and help avoid successful attacks going forwards through shared intelligence and best practice

## Cross-Sector Collaboration

The network is similar to information sharing forums operating successfully in other sectors. It intends to work collaboratively with such groups to benefit from wider threat intelligence

## Regular Engagement

Meetings are likely to occur around four times per year, with additional sessions scheduled as important events dictate an urgent need to share intelligence

# CFISN Event Proforma

**PASA CYBERCRIME AND FRAUD INFORMATION SHARING NETWORK**

**"PROFORMA"**

Submission Template to Support Confidential and Structured Information Exchange

Legal and Confidentiality Reminder:
***The purpose of the CFISN is to facilitate members to share information and to discuss best practice regarding the identification and assessment of, and response to cybercrime and fraud risks. It is imperative that while doing so members fully respect their legal and regulatory obligations, including concerning the privacy of individuals and organisations.***

***Please do not include any personal, confidential, or company-identifiable information in this proforma, including that which relates to an organisation's confidential legal or regulatory reporting obligations.***

## EVENT OVERVIEW

Event Title/Short Description: [Provide a concise, non-identifying summary of the event.]

Date/Time of Event: [Specify when the event occurred—use a general timeframe if necessary.]

Event Type: [Select one: Cyber Incident / Fraud Event / Other (Specify)]

Primary Impacted Domain: [E.g. Finance, Operations, Customer Data, etc.]

Event Detection Method: [How was the event detected?]

# CFISN Event Proforma

## DETAILS OF MALICIOUS ACTIVITY

Means, Methods, and Resources Used by Malicious Actor: [Describe the primary tools, techniques, tactics, procedures or resources that were observed or are suspected to have been used by the malicious actor. Ensure no information is included that could identify the company involved.]

Origin/Entry Point of Event: [Identify the method used to gain entry into the environment (e.g., phishing email, compromised website, social engineering via phone or service desk, physical access, postal delivery, etc.).]

## CYBER EVENT (IF APPLICABLE)

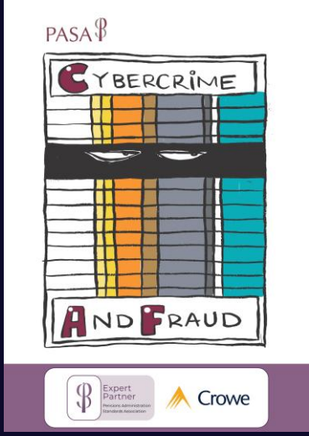
Please refer to MITRE ATT&CK® to support identification of standard Tactics, Techniques, and Procedures (TTPs) that will enable consistent reporting and support the PASA CFISN to consider potential mitigations to be shared to members.

Event described: [Provide a detailed account of the incident, ensuring clarity and specificity while avoiding any information that could identify the company involved.]

MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs): [List relevant MITRE ATT&CK IDs, names, or descriptions as applicable (e.g., Initial Access [T1078], Lateral Movement [T1021], etc.]

Suspected or Known Motivation: [Summarise any known or suspected drivers behind the incident (e.g., financial gain, competitive advantage, operational disruption, etc).]

Observed or Potential Mitigations: [Detail any mitigation measures that were applied or are advised, such as product patches, process improvements, enhanced user training, or stricter access controls etc.]



# CFISN Event Proforma

## FRAUD EVENT (IF APPLICABLE)

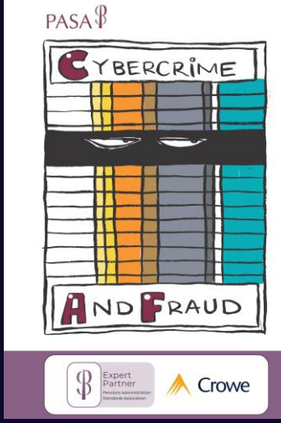
Please refer to All categories A-Z of fraud | Action Fraud to support identification of standard Tactics, Techniques, and Procedures (TTPs) that will enable consistent reporting and support the PASA CFISN to consider potential mitigations to be shared to members

Event described: [Provide a detailed account of the incident, ensuring clarity and specificity while avoiding any information that could identify the company involved.]

Fraud Techniques Employed: [Outline the specific methods used to carry out the fraud (e.g., invoice manipulation, identity impersonation, document forgery, unauthorized account access, etc.).]

Suspected or Known Motivation: [Summarise any known or suspected drivers behind the incident (e.g., financial gain, competitive advantage, operational disruption, etc).]

Mitigation Measures (Observed or Recommended): [Describe the actions taken or proposed to prevent recurrence, such as process enhancements, increased user awareness, policy updates, or technical controls.]



# CFISN Event Proforma

## IMPACT AND RESPONSE

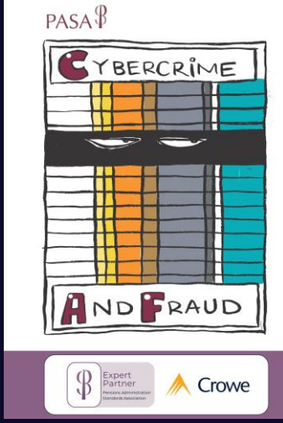
Level of Impact: [Outline the extent of the incident, including the number of affected systems, types of data involved, and any operational disruptions or business impacts.]

Response Actions Taken: [Summarize the key actions taken in response to the event, such as containment steps, system recovery, communication efforts, and any immediate mitigations.]

## LESSONS LEARNED AND RECOMMENDATIONS

Key Findings: [Summarise lessons learned from the event, focusing on detection, response, or prevention. If there are sharable technical indicators of compromise or red flags that can support other members identify similar please include here.]

Recommendations for Others: [Share actionable suggestions or proven best practices to help other PASA members proactively prepare for and reduce the risk of encountering similar.]



# An example of a fraud incident

| | | |
|---|---|---|
| **The incident** | **What happened** | • Identity fraud and impersonation of members to divert pensions |
| | **Tactics involved** | • Bank detail and address changes of multiple members<br>• Rapid retirement requests<br>• Overseas IP access |
| | **Motivations** | • Financial gain |
| | **Mitigation measures** | • Initial fraud monitoring flags raised<br>• Enhanced due diligence<br>• Peer review of high risk cases |
| **Impact & response** | **The impact** | • Member re-verification failures<br>• One payment released |
| | **Response actions taken** | • Admin team on high alert<br>• Investigation team alerted<br>• Report made to law enforcement |
| **Lessons learned** | **Key findings** | • Increased number of fraudulent requests received<br>• High standard of false documentation provided |
| | **Recommendations for others** | • Review of member Identity Verification (IDV) processes - digital ID verification<br>• High risk escalation procedure triggers to be reviewed<br>• Identity document metadata reviews<br>• Admin team awareness and education |

# An example of a cyber incident

| | | |
|---|---|---|
| **The incident** | **What happened** | • Threat actor gained access via compromised admin credentials |
| | **Tactics involved** | • Social engineering via email phishing<br>• MFA fatigue |
| | **Motivations** | • Harvest member data and enable downstream identity and payment fraud |
| | **Mitigation measures** | • Security monitoring flagged abnormal login patterns and impossible travel activity<br>• High-volume data queries outside normal administrator working hours<br>• Endpoint telemetry showed suspicious OAuth token creation<br>• Incident escalated through the SIEM and cyber response playbook |
| **Impact & response** | **The impact** | • Data breach requiring full investigation<br>• Report to data controller/Trustees<br>• Report to ICO |
| | **Response actions taken** | • Incident response procedures and playbook followed<br>• Immediate credential reset and forced logout of affected accounts<br>• Conditional access rules tightened and MFA challenges reconfigured<br>• Compromised endpoints isolated and forensic imaging performed |
| **Lessons learned** | **Key findings** | • Pension data is a high-value target even without immediate cash access<br>• Reputational damage inflicted<br>• Employee awareness and training  must continue to evolve |
| | **Recommendations for others** | • Phishing-resistant MFA is critical<br>• Cyber, fraud and operations teams must share early warning indicators<br>• Regular red-team testing improves detection of credential-based attacks |

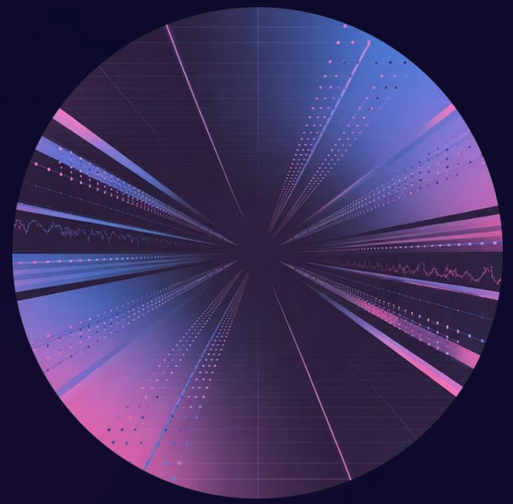
# Who Can Get Involved

## PASA Corporate Members

Representatives from PASA corporate members can join the forum. PASA members cover a wide range of bodies who operate or interact with pensions administration across the UK

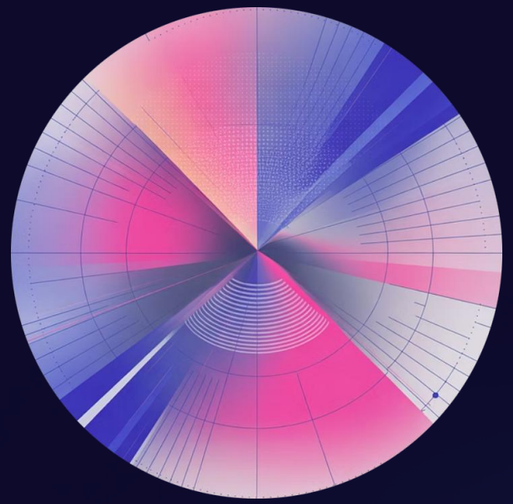
## Cyber Security Specialists

Organisations can nominate representatives who have specialisms in cyber security, bringing technical expertise to the network discussions



## Fraud Specialists

Representatives with expertise in fraud detection, prevention and investigation are particularly valuable to the network.



## Senior Leadership

Senior representatives of organisations who understand the strategic importance of cyber and fraud resilience

**PASA is actively seeking members to join the forum. Your organisation's participation will strengthen the collective defence of the UK pensions industry and protect millions of scheme members.**

# How to Get Involved

## Why Join Now?

- Gain early access to threat intelligence
- Learn from anonymised incident reports
- Share your own experiences confidentially
- Access expert guidance on incident response
- Collaborate with industry peers
- Strengthen your scheme's defences
- Raise resilience in the sector through best practice

*"Collective intelligence is our strongest defence. Together, we can protect scheme members, preserve trust and ensure the resilience of UK pensions administration."*

***Tim Robinson, Partner, Cyber Resilience and Counter Fraud***
***Crowe UK – PASA's Expert Partner for Cybercrime & Fraud***

**Register to join the network by emailing us at CFISN@pasa-uk.com.**

**Start sharing details of incidents with us now – old or new/ongoing – via the same email address.**

**Join our first meeting – Microsoft Teams call to be held on Wednesday 15th July 2026, 10:00 – 11:30.**

**The time to act is now. Cyber criminals and fraudsters are constantly evolving their tactics. By joining the CFISN, you're taking a proactive step to protect your schemes, your members, and the wider pensions industry.**