



Economic and Cyber Crime Committee of the City of London Police Authority Board

Date: TUESDAY, 4 NOVEMBER 2025

Time: 11.00 am

Venue: COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL

Members:

Tijs Broeke (Chair)	Naresh Hari Sonpar
Deputy Madush Gupta (Deputy Chair)	Mandeep Thandi
Melissa Collett	Deputy James Thomson CBE
Alderman Professor Emma Edhem	James Tumbridge
Jason Groves	Deputy Dawn Wright
Andrew Lentin (External Member)	

Enquiries: Sorrel Cooper
Sorrel.Cooper@cityoflondon.gov.uk

Accessing the virtual public meeting

Members of the public can observe all virtual public meetings of the City of London Corporation by following the below link:

<https://www.youtube.com/@CityofLondonCorporation/streams>

A recording of the public meeting will be available via the above link following the end of the public meeting for up to one civic year. Please note: Online meeting recordings do not constitute the formal minutes of the meeting; minutes are written and are available on the City of London Corporation's website. Recordings may be edited, at the discretion of the proper officer, to remove any inappropriate material.

Whilst we endeavour to livestream all of our public meetings, this is not always possible due to technical difficulties. In these instances, if possible, a recording will be uploaded following the end of the meeting.

Ian Thomas CBE
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

2. **MEMBER'S DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**

3. **MINUTES**

To agree the public minutes and non-public summary of the meeting held on 8 September 2025.

For Decision
(Pages 5 - 10)

4. **POLICING PLAN PERFORMANCE REPORT – Q2 2025/26**

Report of the Commissioner.

For Information
(Pages 11 - 38)

5. **SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA – Q2 2025/26**

Report of the Commissioner

For Information
(Pages 39 - 44)

6. **CYBER GRIFFIN UPDATE**

Report of the Commissioner

For Information
(Pages 45 - 48)

7. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

8. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

9. **EXCLUSION OF THE PUBLIC**

MOTION - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following item(s) on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

For Decision

Part 2 - Non-Public Agenda

10. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the meeting held on 8 September 2025.

For Decision
(Pages 49 - 52)

11. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**

Joint report of the Town Clerk and the Commissioner

For Information
(Pages 53 - 70)

12. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE – REGULAR PROGRAMME PROGRESS REPORT**

Report of the Commissioner.

For Information
(Pages 71 - 84)

13. **DOMESTIC CORRUPTION UNIT QUARTERLY UPDATE**

Report of the Deputy Commissioner

For Information
(Pages 85 - 88)

14. **ECONOMIC AND CYBER CRIME ACADEMY RECOVERY PLAN**

Report of the Deputy Commissioner

For Information
(Pages 89 - 96)

15. **ACTION TRACKER**

Report of the Commissioner.

For Information

16. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
17. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

**ECONOMIC SECURITY AND CYBER CRIME COMMITTEE OF THE CITY OF LONDON
POLICE AUTHORITY BOARD
Monday, 8 September 2025**

Minutes of the meeting of the Economic Security and Cyber Crime Committee of the City of London Police Authority Board held at Committee Rooms, 2nd Floor, West Wing, Guildhall on Monday, 8 September 2025 at 10.00 am

Present

Members:

Deputy Madush Gupta (Deputy Chair)
Melissa Collett
Andrew Lentin (External Member)
Naresh Hari Sonpar
Mandeep Thandi
Deputy James Thomson CBE
Deputy Dawn Wright
Jason Groves

Officers:

Richard Riley	- Town Clerk's Department
Oliver Bolton	- Town Clerk's Department
Ben Dunleavy	- Town Clerk's Department
Cyra Mutesi	- Town Clerk's Department
Melissa Panszi	- Innovation & Growth

City of London Police:

Nik Adams	- City of London Police
Tor Garnet	- City of London Police
Blair Stringman	- City of London Police
Chris Bell	- City of London Police
Carly Humphries	- City of London Police
Matthew Bradford	- City of London Police
Lucy Cumming	- City of London Police

1. APOLOGIES

Apologies were received from the Chairman Tijs Broeke, Alderwoman Emma Edhem and James Tumbridge. All three Members observed the meeting virtually.

2. MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA

There were no declarations.

3. MINUTES

RESOLVED - That the public minutes and non-public summary of the meeting on the 20 May 2025 be approved as an accurate record.

4. **QUARTER 1 - NATIONAL LEAD FORCE CITY OF LONDON POLICE PERFORMANCE REPORT**

The Committee received a report of the Commissioner with an assessment of City of London Police performance against the objectives set out in the National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28 for quarter 1 2025/26 (1 April 2025 – 30 June 2025).

Members noted that the force had achieved a 44% year-on-year increase in disruptions against organised crime groups (OCGs), recording 513 disruptions and 39 pocket activities for the quarter, demonstrating a strong start to the year. Home Office targets for protecting people and businesses were met.

Economic cybercrime was highlighted as an area of concern, with training levels at the Economic Cyber Crime Academy having declined over a two-year period. This was due to financial pressures, accreditation requirements, and reduced cost competitiveness. Work was underway to diversify training audiences, explore additional funding, and expand international delivery, including courses for officers in Mauritius and Nigeria.

A Member raised concerns about the temporary impact on performance of staff reassigned to support the new Action Fraud system. Officers confirmed this had resulted in a temporary reduction in priority allegations and some performance metrics; this was anticipated and within tolerance. The new system was expected to improve linking of related reports, reduce manual bottlenecks, and enhance case management, victim communication, and investigative outcomes once fully operational.

A Member asked about activity relating to OCGs and the Proceeds of Crime Act (POCA). Another Member enquired on training throughput, academy attendance, and declining domestic uptake. Members also asked about reporting timing and format - including colour coding and consolidation of performance packs - allocation of officers to the Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS), consistency in statistics, and the use of artificial intelligence (AI) and flexible training models.

Officers highlighted ongoing international and financial sector training, collaboration with UK Finance and the National Crime Agency (NCA), and initiatives to improve operational effectiveness. Members noted improvements in contact centre performance, with average wait times reducing substantially over the last two years.

A Member requested a concise crib sheet summarising key metrics and benefits from the report, to support discussions with colleagues and stakeholders. Officers confirmed that, while some benefits were not yet fully realised, a short summary would be prepared and made available to Members by 4 September.

RESOLVED - That the report be noted.

5. **POLICING PLAN PERFORMANCE REPORT - Q1 2025/26**

The Committee received a report of the Commissioner with an assessment of City of London Police performance against the objectives set out in the Policing Plan for quarter 1 2025/26 (1 April 2025 – 30 June 2025).

Members noted that this was the first time that Policing Plan ('the Plan') metrics were being reviewed upfront. Officers highlighted efforts to extract key measures that reinforce the Plan without duplicating reporting. A Member asked how often the Committee would review different performance measures going forward; officers confirmed that this would be considered in designing future reporting cycles.

Members welcomed the continued rollout of the National Economic Crime Victim Care Unit (NECVCU), with Level Two services now being provided to 38 forces, up from six previously, and nearing coverage of the full 43-force population. Officers explained that discussions were ongoing with the remaining forces, some of which had mature supply chains or existing contracts, to ensure continued evolution towards full network adoption. Members acknowledged the value of City of London Police leadership in achieving this network impact.

A Member requested that the full results analysis, including complaints data, be summarised for the next meeting. Officers confirmed that operational details would not be shared, but outcome-focused information, such as the percentage alongside complaint volumes, would be provided to allow Members to monitor trends effectively.

Members also noted encouraging returns from victim surveys, indicating that victims feel safer following contact with an advocate. The timeline for FCCRAS was highlighted, with officers noting that the programme was approaching completion after many challenging years.

Finally, Members observed that with the refocus of performance sections in line with recent governance changes, coverage of the Cyber programme, including Cyber Resilience Centres (CRCs), had been reduced. Officers confirmed that this would be addressed in future agenda packs.

RESOLVED - That the report be noted.

6. SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA - Q1 2025/26

The Committee received a report of the Commissioner with an assessment of City of London Police performance against the objectives set out in the Policing Plan for quarter 1 2025/26 (1 April 2025 – 30 June 2025).

Members noted that this was the first time complaints data relating to Action Fraud had been presented to the Committee, having previously being considered by the then Professional Standards and Integrity Committee (now the Professionalism and Trust Committee). The number of complaints remained extremely low, at approximately 0.08% of reports, which was consistent with previous quarters, and primarily related to frustrations about reports not being investigated rather than concerns with the reporting service itself.

Members discussed improvements to the victim journey, noting that the replacement system for Action Fraud will allow victims to log in and track their case progress, with automated updates provided across 46 trigger points, compared with three previously. The system also ensured clear communication when cases were not pursued for investigation and highlighted how information provided by victims was used to disrupt

criminal activity and prevent repeat victimisation. Members emphasised the importance of monitoring public perception and outcomes as the system was rolled out, to inform evaluation and external communications.

Members also welcomed the continued rollout of the National Economic Crime Victim Care Unit (NECVCU), with Level Two services now provided to 38 forces, approaching full coverage of the 43-force network. Officers highlighted ongoing engagement with the remaining forces, some of which have mature supply chains or existing contracts, to ensure wider adoption.

A Member requested that future reports provide outcome-focused information alongside complaint volumes, including percentages, to allow trends to be effectively monitored.

RESOLVED - That the report be noted

7. INNOVATION & GROWTH - UPDATE OF CYBER & ECONOMIC CRIME RELATED ACTIVITIES

The Committee received a report of the Executive Director, Innovation and Growth (IG), providing an update on the department's work on digital verification, cybersecurity talent, and anti-money laundering.

Members noted that the Police Authority team continued to work closely with IG colleagues to identify opportunities to promote the role and interests of the City of London Police, particularly its National Lead Force for Fraud responsibilities. The Police Authority team also sought opportunities to highlight IG's work on digital verification, recognising its potential impact on combating fraud.

Officers outlined collaborative work undertaken by the City Corporation, including advocacy with key stakeholders, such as correspondence with the Governor of the Bank of England, and participation in high-profile dinners hosted by the Lord Mayor for the financial, professional services and technology sectors. These engagements had reinforced the strategic role of the police and provided a platform to promote the City Police's economic and cyber crime initiatives.

Members were briefed on digital verification initiatives, which aim to increase adoption of effective verification processes. A roundtable in July explored the mass-market landscape and requirements for scaling a UK digital verification orchestrator. Officers confirmed that a steering committee was being established with representatives from industry, government, and academia, with a view to launching a working group by the end of October.

On anti-money laundering, Members were informed that IG and the Police Authority Board had hosted the launch of a Financial Action Task Force report in March.

Members welcomed the focus on digital verification and highlighted the wider relevance to national security and the financial sector.

A Member highlighted the economic security implications of recent high-profile cyber-attacks and their potential financial impact on City businesses.

Members encouraged IG to explore opportunities for the Corporation to provide unique insight into these impacts.

RESOLVED - That the report be noted.

8. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

There were no questions.

9. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**

Members were updated on the ministerial reshuffle announced on 5 September 2025.

Shabana Mahmood replaced Yvette Cooper as Home Secretary, while Sarah Jones and Alex Norris were appointed to roles within the Home Office covering immigration and policing, with specific portfolios yet to be confirmed.

Members noted that these ministers were not new contacts, with previous engagements including a visit by Sarah Jones to the City of London Police in September 2023 and a meeting with Alex Norris in February 2024 during his tenure as Shadow Policing Minister. Dan Jarvis remained Security Minister with an additional Cabinet Office portfolio, and Lord Hanson continued as the Minister covering fraud.

RESOLVED - That the update be noted.

10. **EXCLUSION OF THE PUBLIC**

RESOLVED - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the meeting for the following item(s) on the grounds that they involve the likely disclosure of exempt information as defined in Part I of Schedule 12A of the Local Government Act.

11. **NON-PUBLIC MINUTES**

RESOLVED - That the non-public minutes of the meeting held on 20 May 2025 were approved as an accurate record.

12. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**

The Committee received a joint report of the Town Clerk and The Commissioner on the Strategic Communications and Engagement Plan for Economic and Cyber Crime.

13. **NATIONAL DOMESTIC CORRUPTION UNIT**

The Committee received a report of the Commissioner on the National Domestic Corruption Unit (DCU), providing a summary update on the pilot programme and the associated Anti-Corruption Strategy.

14. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**

There were no questions.

15. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**

There was no other business.

The meeting ended at 11.58 am

Chairman

Contact Officer: Ben Dunleavy
ben.dunleavy@cityoflondon.gov.uk

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee	Dated: 4 November 2025
Subject: Policing Plan Performance Report – Q2 2025/26	Public Report: For Information
This proposal: <ul style="list-style-type: none"> • Delivers Corporate Plan 2024-29 outcomes • Provides statutory duties 	<ul style="list-style-type: none"> • Diverse Engaged Communities • Dynamic Economic Growth • Vibrant Thriving Destination • Providing Excellent Services
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£-
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Commissioner of City of London Police
Report author:	T/Ch Insp Megan Cardy, Head of Force Performance

Summary

The appendix to this cover report summarises the Policing Plan Performance for Q2 in 2025/26. The appendix provides an overview of the City of London Police performance and National Delivery Plan Performance.

Recommendation(s)

Members are asked to:

- Note the report.

Appendices

- Appendix 1 – City of London Policing Plan Performance Report Q2 – 2025/26
- Appendix 2 – National Delivery Plan Performance Report Q2 – 2025/26

T/Ch Insp Megan Cardy

Head of Force Performance, Corporate Services

This page is intentionally left blank

National Lead Force City of London Police Performance Report

Page 13
H
Q2: July – September 2025



Performance Assessment

The dashboard provides an assessment of City of London Police performance against the objectives set out in the **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28**. The National Policing Strategy was launched in November 2023 and translates national strategies and objectives set by His Majesties Government into actionable measures for policing in the areas of fraud, money laundering and asset recovery and cyber. The report shows CoLP attainment against the objectives. The National Policing Strategy sets out a purpose to “improve the UK policing response to fraud, economic and cyber crime” through three **key cross cutting objectives** of:

- Improving outcomes for victims;
- Proactively pursuing offenders;
- Protecting people and business from the threat of Fraud, Economic and Cyber Crime.

The NLF plan sets out key cross cutting enabling commitments that City of London Police is seeking to achieve:	FYTD Performance	Data Trend
We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.		↑
We will deliver enhanced victim care & support to victims of fraud & cyber crime, to reduce harm of offending and prevent re-victimisation.		↑
We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.		⇒
We will improve the policing response to fraud. Fraud and Cyber Reporting and Analysis Service (FCCRAS) objectives will be added when the system launches.		↑
We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages		↑
We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.		↑
We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber crime.		↓
We will develop and action a National Economic Crime Workforce Strategy.		↑

Executive Summary: Key Cross Cutting Strategic Objectives



There have been significant number of outcomes for victims this quarter due to one investment fraud investigation successfully charging a number of suspects. This has been a significant investigation for one of COLP's National Fraud Operations Teams.

The nature of COLPS investigations mean these significant investigations do have an impact on the fluctuation of outcome rate for COLP. Judicial Outcome Rate for CoLP now remains significantly above the national average of (19%).

The Victim Care Unit, in addition to increasing the victims contacted as part of ongoing investigations are also improving how they offer protect advice to the victims they engage with and have begun seeking feedback on how useful that advice and the overall service has been for victims.

CoLP has not met its target relation to training of fraud investigators in Q1 and Q2, however work is ongoing to increase delegates by increasing accessibility of courses to colleagues who cannot attend a venue in person.



NLF continued to disrupt serious and organised fraud and cyber offending this quarter with significant disruptions to Organised Crime Groups (OCGs), through the apprehension and conviction of suspects as well as the successful restriction of their assets.

The use of financial investigation powers against offenders has also increased this quarter – this is a positive way to disrupt offending whilst criminal investigations continue and can lead, as they did this quarter, to funds being repatriated to victims at the successful conclusion of criminal proceedings.

Industry disruptions have increased this quarter which is positive given the low levels recorded in Q1. They do significantly vary based on investigation types and the identification of information that can lead to disruption.



The volume of protect engagement continues to increase positively however attendees decreased, this is in line with seasonal trends and are expected to pick up in Q3.

COLP is looking to improve its understanding of the impact of the repeat victims by looking right across the reporting picture at repeat victimisation trends to help inform the new focussed efforts on areas where protect engagements really have impact.

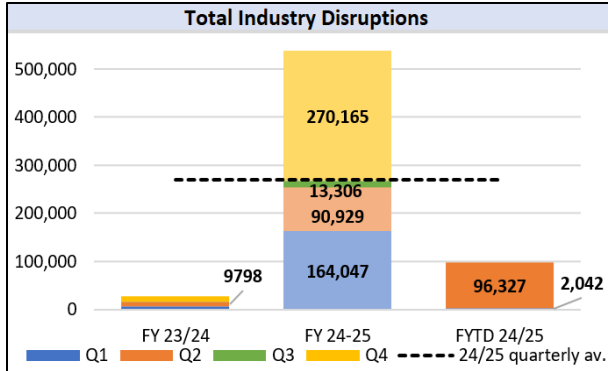
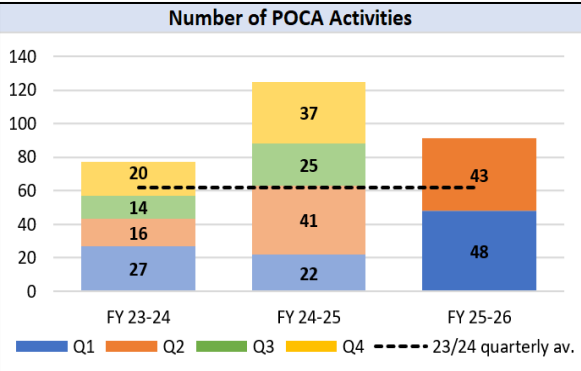
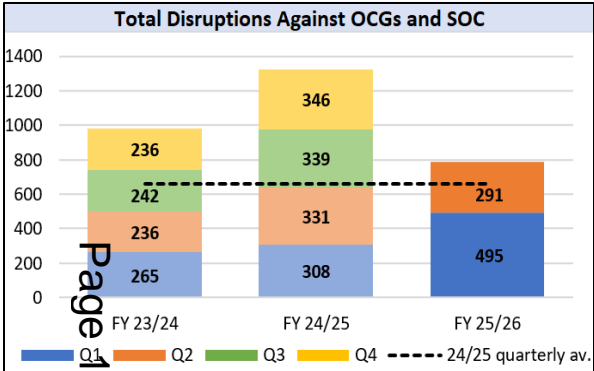




We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:

A. Increase the number of disruptions against fraud organised crime groups (OCG) and serious organised crime (SOC)		↑
B. Increase the number of POCA activities		↑
C. Increase the number of disruptions against technological enablers		↓



OCG Disruptions

- Teams are investigating **68** OCGs (-5)
- In Q2 teams recorded against OCGs:
- 3 major** disruptions (-2 to 24/25 Q1)
- 10 moderate** (-4 on 24/25 Q1)
- 27 minor** disruptions (+20 on 24/25 Q1)
- 251** disruptions against other threats is a **24% (+187)** increase on Q2 24/25
- Total disruptions against OCGs and SOC for the first half of the year are up **23% (+147)** from Q1 & 2 24/25, which is in line with the 5-year trend

Financial Disruptions

- In Q2 25/26 Fraud Teams reported **43** POCA activities up **5% (+2)** from Q2 24/25 and 39% (+12) from the quarterly avg.
- These had a value of **£1,134,668** down **65% (-£2,122,250)** from Q2 24/25 and down 51% (-£1,198,771) from the quarterly avg.
- Activities included: **7** confiscations, **2** asset restraining orders, **27** cash detentions and **7** cash forfeitures
- 178** victims were awarded a share of **£146,089** in compensation

Industry Disruptions

In Q2 Fraud teams reported:

- 448** disruptions to websites
- 95,873** to cards and bank accounts
- 6** to social media accounts
- 5% (+4,944)** increase on total disruptions compared to Q2 24/25

Response Industry Disruptions

In Q2 there were increases across all types of disruption, particularly against bank accounts with **DCPCU** recording large volume disruptions in July (prolific 'smisher') and September (courier fraud and selling of account data).

Response

OCG Disruptions

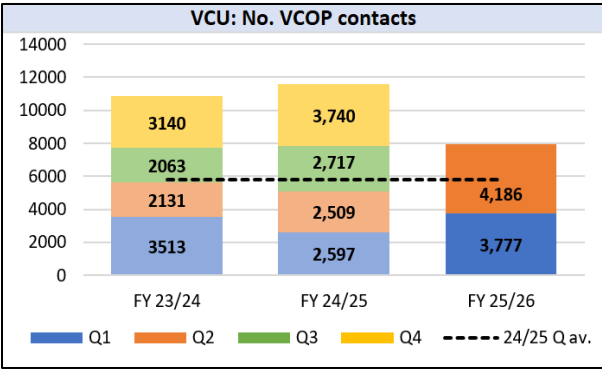
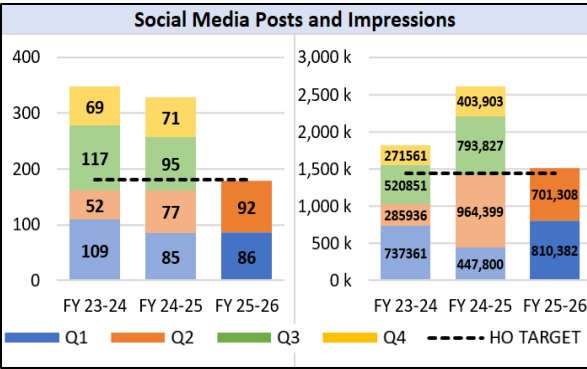
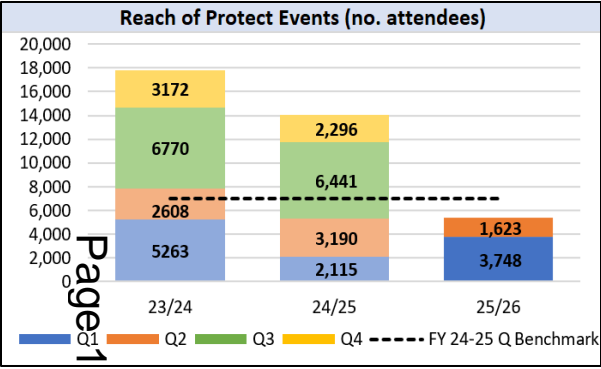
PIPCU targeted counterfeit football merchandise in operations with partners. 7 individuals were arrested, and 329 fake football kits and 184 pairs of counterfeit football socks were seized. The operations followed intelligence from the IPO regarding sale of fake football merchandise.

Financial Disruptions

An OCG which ran bogus investment schemes and coerced 150 victims out of £6 million was disrupted with the sentencing of the leader for 7.5 years in prison, having pleaded guilty to conspiracy to defraud, money laundering and perverting the course of justice. His co-defendants were also found guilty. More than £2 million of the stolen money has been returned to the victims. A **Money Laundering** DC used civil and criminal charges to accomplish the outcome. A man who pocketed £1 million by running 3 illegal streaming websites has been jailed for 3 years. **PIPCU** secured an all-assets restraint order against £1.1 million held in bank accounts and cryptocurrency wallets. These funds, will now be subject to confiscation proceedings.

We will deliver enhanced victim care and support to victims of fraud and cyber crime, to reduce harm of offending and prevent re-victimisation. We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.

Success Measures:		
A. Increase the number of protect engagements and attendees		↓
B. Increase the number of social media posts and impressions – Home Office Measure		⇒
C. Increase the number of Victim Care Unit contacts		↑



Protect Events

- Teams held **37** events in Q2 up over **100% (+19)** from Q2 24/25
- 1,623** people attended these events up **49% (-1,567)** from Q2 24/25
- Activity peaked in Sept after summer breaks with **16** events & **852** attendees

Response Protect Events

The DCPCU Protect team delivered 8 training sessions in July to over 325 people, covering a range of topics. They also hosted the 1st Virtual Industry Visit where they opened the sessions to wider audiences to widen the knowledge base.

Social Media – HO Measure

- Teams posted **92** messages on social media, up **19% (+15)** on Q2 24/25
- The related impressions fell slightly to **701,308**, down **21%** on Q2 24/25, which was the highest return in the last 3 years due to a press release regarding a high-profile retail fraud investigation
- Posts and impressions were particularly high in July with a large number of press releases issued by Corporate Communications
- Home Office target Met**

Victim Care Unit

- VCU was responsible for **5,679** victims in Q2 up **25% (+1,123)** victims since Q2 24/25 relating to **27 (+4)** investigations
- A total of **4,186** VCOP updates were issued, up **45% (+1,677)** from Q1 24/25
- 3,965** victims received additional Protect advice

Response Victim Care Unit

The number of cases and victims covered by VCU has risen over the last year, thus giving a rise in VCOP contacts. Additionally in July, VCU sent additional prevention advice on behalf of Leicestershire Police.

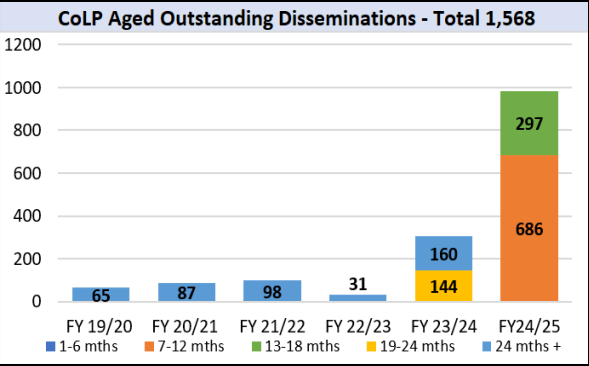
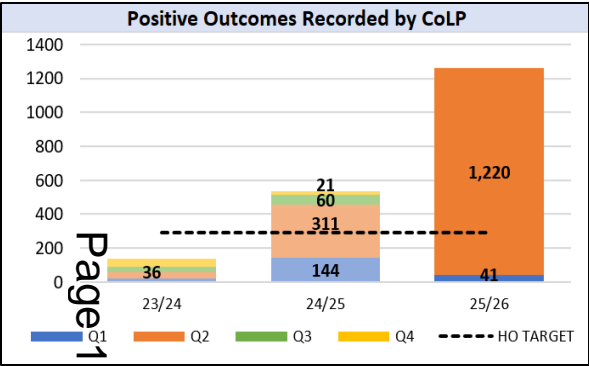
Response Social Media

- PIPCU** issued an appeal for help from the public to trace a woman wanted in connection with the illegal selling of counterfeit weight loss medications which attracted extensive media coverage.
- IFED** posts focused on their ‘crash for cash’ intensification along with high profile sentencings.
- NLF Ops** posted about the national courier fraud campaign with DSI Little appearing on Good Morning Britain.
- DCPCU** saw an increase in impressions and engagement via LinkedIn. Their post with the highest engagement rate was a weekly round up featuring photos including ‘digi dog’ Barney.

Upcoming in Q3: October is National Cyber Security month, and posts will support the upcoming courier fraud intensification. In November focus will be on Black Friday and Cyber Monday related frauds before moving to the 12 Frauds of Christmas in December.

We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.

Success Measures:		
A. Increase the positive outcome rate for CoLP – Home Office Measure		↑
B. Decrease CoLP aged outstanding disseminations		↓
C. Support CoLP teams to engage in intensification efforts – Home Office Measure		↑



Positive Outcomes – HO Measure

- In Q2 CoLP teams recorded **1,220** positive outcomes
- Up **292% (+909)** from Q2 24/25, which was also a high yielding quarter
- 101** no further action outcomes were also recorded, contributing to the fall in Aged Outstanding Disseminations
- The positive outcome rate (positive outcomes divided by all outcomes) was **92%** for Q2, an increase from **83%** in Q2 24/25
- Home Office target exceeded**

Outstanding Disseminations

- At the end of Q2 **1,568** disseminations from 19/20 to 24/25 were with CoLP teams awaiting outcomes
- This is down **25% (-534)** from the end of Q1 showing ongoing improvement and the impact of closing one large investment fraud case

Intensifications – HO Measure

Operation Haechi is an initiative developed by South Korean Police and led by the Interpol Financial and Anti-Corruption Centre (IFACC). The aim is to recall funds sent internationally as a result of fraud. The National Central Bureau Manchester and the CoLP IDT are jointly leading the UK response.

Op Haechi VI took place from 23/04 to 22/08. Within this period 34 INTERPOL Global Rapid Interventions were released by the intel team. This is a stop-payment mechanism within INTERPOL. 135 referrals were made through Action Fraud overnight submissions.

Op Tonic is an umbrella term used for romance fraud and incorporates national Protect work. A recent intensification ran from 29/09 to align with Romance Fraud Awareness Week and the in-person Date Safe conference. It is hoped there will be a reduction in dating scam reports when analysis takes place.

Home Office target met

Response

Positive Outcomes

In September, CoLP teams recorded their highest ever yield of positive outcomes at 1,220. Of these, 1,199 relate to a single investment fraud investigation by the Fraud Ops Teams. 1,250 investors put £25m into the fraudulent scheme. The investigation took 5 years of tireless work to bring to charging and POCA proceedings are ongoing.

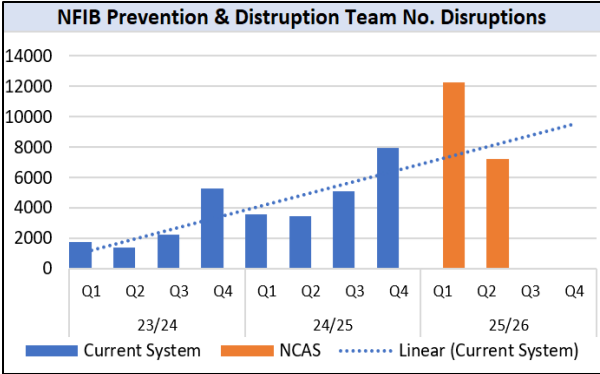
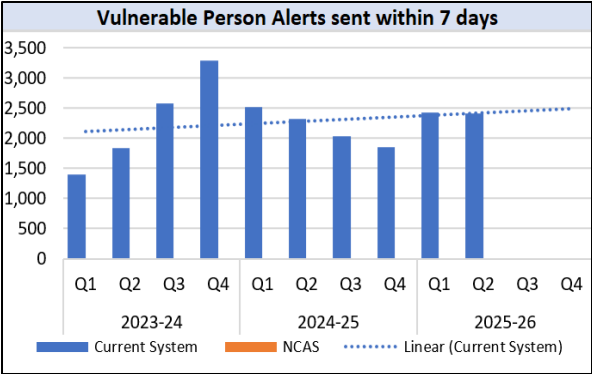
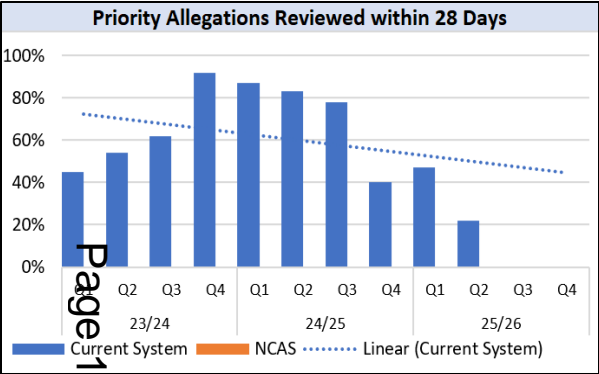
Total CoLP positive outcomes across all units remain flat with circa 12 returns on average a month excluding large one-off operations.

Within the pipeline are three investigations into investment frauds with a combined total of at least 1,200 victims. These are expected to come to a conclusion in 1-2 years.

Total outcomes reported in a period can relate to disseminations from any time. The volume of outcomes fluctuates throughout the year as cases with varying numbers of crimes attached are completed.

We will deliver the Fraud and Cyber Reporting and Analysis Service (FCCRAS) - including the ability to feedback intelligence into the system for further development and inclusion in intelligence packages. We will ensure intelligence is appropriately recorded and disseminated to assist with all 4P outcomes

Success Measures:		
A. Increase the allegations of fraud reviewed in 28 days meeting 'highly likely' & 'likely vulnerable' on the solvability matrix		⬇
B. To review and, where appropriate, disseminate vulnerable person alert within 7 days		⬆
C. Increase the number of NFIB P&D disruptions		⬆



Priority Allegations

- In Q2 25/26 NFIB teams reviewed **22%** or **698** of the 3,355 allegations classified as priority
- This is down **47%** from the **1,311** allegations reviewed in Q2 24/25 which totalled 83% of the priority allegations
- The last three quarters have seen an expected drop due to abstractions, current system latency, downtime and testing of the new operating platform

Vulnerable Person Alerts

- NFIB sent **2,411** vulnerable person alerts to forces in Q2
- This is an increase of **4% (+93)** alerts from Q2 24/25
- Consistently, **99%** of these were sent within the 7-day target timescale showing excellent victim care

The transition of the VPA process to Victim Services is going well, it is still being supported by the NFIB until launch to ensure all victims are safeguarded accordingly and resilience will be built

Preventions and Disruptions

- In Q2 the NFIB P&D team carried out **7,191** disruptions, up **109% (+3,752)** from Q2 24/25.
- Disruptions included:
 - 1,070** website disruptions
 - 1,110** email account suspensions
 - 269** telephone deactivations
 - 4,661** proactive domain suspensions
 - 81** social media account suspensions

Response

NFIB

In Q2 performance continues to be affected by the transition to the new operating system, as a team of 5 remain abstracted from core business to support FCCRAS delivery.

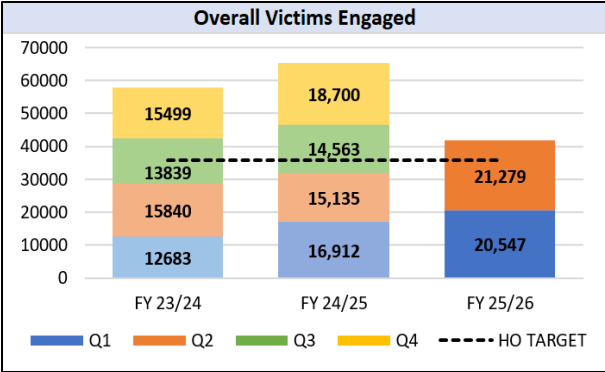
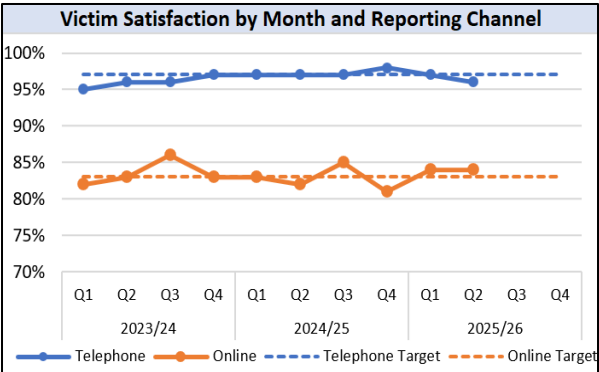
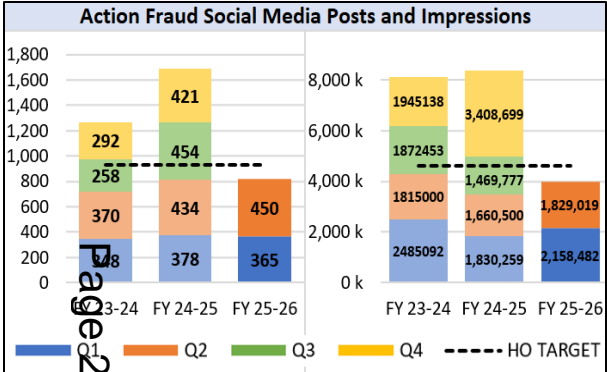
Testing of the system as a whole and of different builds as they finalise within the environment is impacting usual capability. This is set to increase into Q3 due to training large sections of the Crime Team ahead of go live and the end-to-end workflow being tested fully to ensure a smooth user journey.

Current service issues continue, resulting in significant downtime and latency problems; delaying ingests and processing of data for action. We anticipate this reduction in performance to continue until after go live.

The NFIB Disruptions Team are forging ahead with use and development of the National Crime Analysis System (NCAS) showing great returns on disruptions and suspensions.

We will improve the policing response to fraud.
Fraud and Cyber Reporting and Analysis Service (FCCRAS) objectives will be added when the system launches.

Success Measures:		
A.	Increase the number of Action Fraud social media posts and impressions – Home Office Measure	<div></div> ↑
B.	Maintain the percentage of survey respondents who are satisfied with the Action Fraud reporting service – Home Office Measure	<div></div> ⇒
C.	Increase number of fraud victims who receive protect advice (NECVCU engagement) – Home Office Measure	<div></div> ↑



Response

NECVCU

In Q3, Victim Services will implement a new Crime Recording Management System (CRM) designed to streamline administrative tasks and automate processes. During the initial implementation there may be a temporary dip in performance as staff adapt to the new system. However, as confidence and proficiency grow, the CRM is expected to enhance efficiency and overall service delivery. The new technology will allow us to record repeat victims for the level 1 service giving additional insight that current technology does not allow for.

Victim Services will soon be providing a consistent service to all persons who report to Report Fraud across England and Wales, ending previously agreed local exceptions. This change ensures an equitable service for all victims, removing regional disparities and ensuring each report is handled in-line with Victim Services’ policies and procedures.

Action Fraud Social Media – HO Measure

- AF made **450** posts in Q2, up **4% (+16)** from Q2 24/25 and a return to form from Q1 25/26
- The related impressions for these posts totalled **1,829,019** an increase of **10% (+168,519)** from the previous year but below the Home Office stretch target
- **Home Office stretch target not met**

Response Action Fraud Social Media

AF supported the Home Office phishing campaign through the summer. Analysis shows that within a month of the launch reporting of this fraud was up 23.8%.

Action Fraud Satisfaction – HO Measure

- Contact Centre satisfaction was at **96%** in Q2, 1% below the Home Office target
- Online reporting remained at **84%**, **1%** higher than the Home Office target
- Call abandonment was at 22%, and average call waiting time at 4.59 minutes, both improving on 24/25
- **Home Office Target met**

Response Action Fraud satisfaction

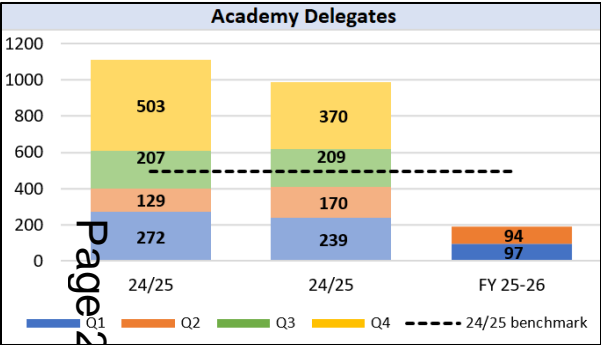
A new reporting tool, designed to improve reporting mechanisms, will launch in 2025. It is envisaged this will bring online satisfaction in line with voice satisfaction.

NECVCU Victim Contacts – HO Measure

- NECVCU engaged **21,279** victims, up **41% (+6,144)** from Q2 24/25 and **18% (+3,318)** on the Home Office target
- Level 1 engagements rose by **42% (+5,293)**
- Level 2 engagements rose by **32% (+851)**
- **0.29%** repeat victims (meets HO target)
- **79%** of victims felt confident online after engagement (meets HO target)
- **Home Office engagement target met**

We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber crime. We will roll out a revised performance framework across PURSUE, PROTECT, PREPARE and PREVENT. ROCUs and Forces to ensure completion of performance framework and resulting recommendations. We will invest in and explore technological and data sharing solutions and opportunities.

Success Measures:		
A.	To increase delegate training levels in the Economic and Cyber Crime Academy (ECCA).	<div></div> ↓
B.	Deliver objectives against National Workforce Strategy.	<div></div> ↑
C.	Provide forces who are due to be inspected with specific pre-inspection support for delivering against the Fraud pillar within the PEEL framework – Home Office Measure	<div></div> ↑



Academy

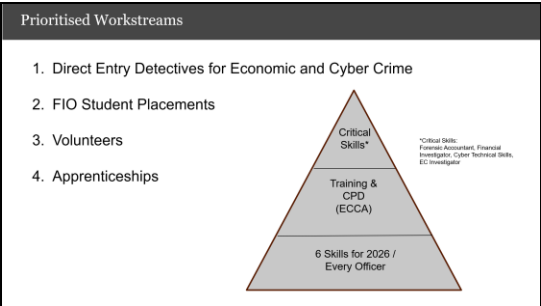
- In Q2 the ECCA held **9** courses, down **36% (-5)** from Q2 24/25
- At **94** delegate numbers were down **45% (-76)** from Q2 24/25
- 90%** satisfaction was equal to Q2 24/25 and the benchmark

Academy

In November, the ECCA is piloting an inclusive training course. An Economic Crime Investigation Foundation course will take place on Teams, to meet the accessibility needs of colleagues who cannot attend a venue in person.

Response Academy

In Q2 bookings continued to be low due to forces and ROCUs having limited budgets. However, CPD training continued its upwards trend. As usual no courses were run in August due to seasonal low uptake. The focus was on preparing and promoting courses planned for the end of the year to ensure strong attendance. Looking ahead, course enrolment figures for October are continuing to rise, indicating strong engagement.



Workforce Strategy

Three workstreams have now been prioritised with updates below:

Direct Entry Detectives. Cohort 1 (D6) officers are now on their rotations within CoLP. Contract signed with Police Now for a second Cohort (D7) on the Economic and Cyber Pathway starting with CoLP in March 2026. This will continue to build the evidence base for the wider national take-up of the scheme.

FIO Student Placements. Cohort 2 (12 students) have now started with CoLP, the MPS, and four ROCUs. Two Students from Cohort 1 are now working part-time. Cohort 2 students will move to part-time in September 2026. Attraction and recruitment underway for Cohort 3, which will consist of 20 students starting with an expanded number of forces and ROCUs in Sept 2026.

Volunteers. Funding agreed through the Cyber portfolio for two secondments (Chief Inspector and Police Staff Deputy) to lead the national programme. Recruitment complete and preferred candidates in vetting and onboarding.

PEEL Support – Home Office Measure

In Q2 the NCO have published a Regional Engagement Report that provides comprehensive detail of the findings with regard to the regional assessments. 73 recommendations flow from the report.

The NCO continue to work with forces in providing guidance and support in expectation of forthcoming HMICFRS visits.

Forces met in Q2: up from 1 in Q1

Dyfed Powys
Essex
Norfolk
Bedfordshire
Lancashire
West Mercia

Home Office measure met

This page is intentionally left blank

National Lead Force National Delivery Plan Performance Report

Page 23
FQ2: July – September 2025



Performance Assessment

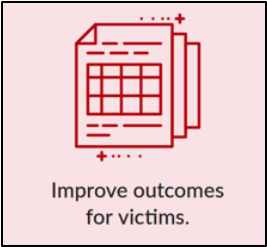
The dashboard provides an assessment of national policing performance against the objectives set out in the **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-28**. The National Policing Strategy was launched in November 2023 and translates national strategies and objectives set by His Majesties Government into actionable measures for policing in the areas of fraud, money laundering and asset recovery and cyber. The report shows national attainment against the objectives. The National Policing Strategy sets out a purpose to "improve the UK policing response to fraud, economic and cyber crime" through three **key cross cutting objectives** of: Improving outcomes for victims; Proactively pursuing offenders; Protecting people and business from the threat

The NLF plan seeks out key cross cutting enabling commitments that City of London Police is seeking to achieve		FYTD Performance	Data Trend
Money Laundering Asset Recovery 1	We will increase disruptions against money laundering offenders.		➡
Money Laundering Asset Recovery 2	We will seize and restrain more criminal assets through including released asset denial activity		⬇
Money Laundering Asset Recovery 3	We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.		⬇
Fraud 1	We will increase the policing response and outcomes linked to National Fraud Intelligence Bureau/ Fraud and Cyber Crime Reporting Analysis System crime dissemination packages.		⬆
Fraud 2	We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The National Fraud Squad teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.		⬆
Fraud 3	We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in National Economic Crime Centre led fraud intensifications throughout the year.		⬆
Fraud 4	We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations.		⬆
Fraud 5	We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.		⬇

Performance Assessment

		FYTD Performance	Data Trend
Cyber 1	We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.		↑
Cyber 2	We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.		↑
Cyber 3	We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.		↑
Cyber 4	We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.		↑
Cyber 5	We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership.		↓
Cyber 6	We will develop improved referral process for new nominals to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.		→
Cyber 7	We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.		↑
Cyber 8	We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.		↓

Executive Summary



The volume of positive outcomes and the positive outcome rate for fraud investigation continues to increase nationally.

COLPs work to reduce the number of outcomes showing as ongoing but without investigative activity has positively impacted this further. The proportion of investigations ongoing has now reached stable levels that are considered reasonable when comparing with other crime types nationally 8% of crime from the past 12 months is open this increases significantly for complex crimes such as Rape where this is 41% and Fraud investigations overall sit within that range appropriately.

The recording of crimes for Computer Misuse Act and Money Laundering offences remains a national challenge and therefore the outcomes of these crimes are not currently possible to meaningfully report on at a national level.

The impact of the transition towards the new recording and analysis system remains this quarter and is impacting capacity of the team and therefore overall crime dissemination volumes. It is likely that some impact will remain for the rest of this reporting year.



The NPCC Serious and Organised Crime portfolio is currently undertaking an APMIS consistency review across all SOC (including fraud and cyber) recorded disruptions.

The team identified that regions and forces are regularly recording effort rather than impact, some regions have already taken proactive action to change this by reviewing both their recording and challenge practices. This has led to lower disruption volumes in a number of different SOC threats in Q2 and is likely to continue to impact disruption volumes going forward as guidance is reissued and other forces and regions carry out internal reviews.

These lower volumes are reflective of recording practice changes rather than a reduction in the action being taken to proactively pursue offenders.



Protect engagement volumes have reduced to levels consistent with 2023/24 as the fraud protect work becomes more focussed in its approach towards engagements where evidence exists to show behaviour change as an output.

The engagements that have been undertaken to protect people and business from both fraud and cyber crime remains really positive with high levels of satisfaction with protect events held this quarter.

As well as focussed events in Q3 based on seasonal crime trends the delivery of the Fraud and Cyber Crime Reporting and Analysis System will further increase COLPs work to protect people from the threat of fraud, economic and cyber crime.

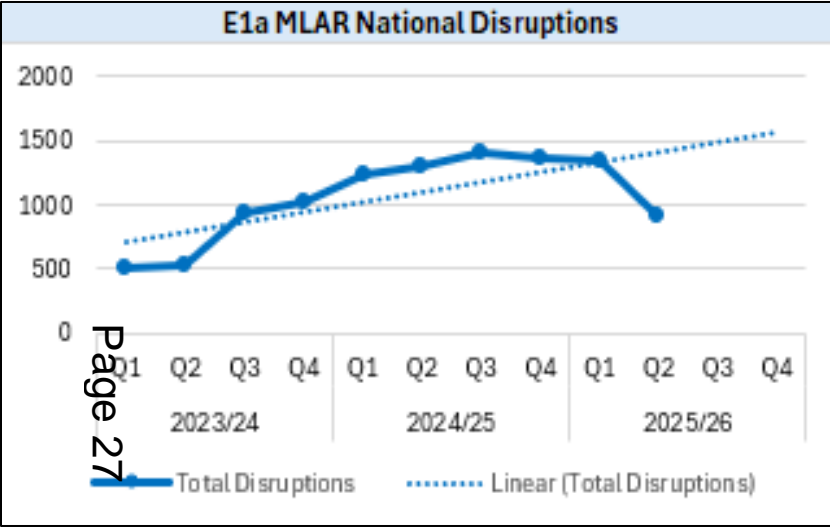
Performance Measure 1: We will increase disruptions against money laundering offenders.

Success Measures:

E1a Increase the number of recorded disruptions linked to money laundering and or illicit finance – **Home Office Measure**

FYTD Performance

Data Trend



Analysis

E1a Money laundering and asset recovery (cash confiscation/cash seizure/recovered assets) is classed as illicit finance on APMIS.

In Q2, there were a total of 906 disruptions.

- 64 major disruptions - 18% decrease (-14) in comparison to Q1 25/26
- 153 moderate disruptions - 35% decrease (-84) in comparison to Q1 25/26
- 689 minor disruptions - 33% decrease (-347) in comparison to Q1 25/26.

The top 3 disruption types are asset denial & ancillary orders at 53% (501), seizures at 20% (192) and investigative suspect disruptions at 10% (93).

In comparison to the previous quarter (Q1), MLAR disruptions are reporting a 33% decrease (-445). In comparison to the same quarter for the previous year (Q2 24/25), there has been a 31% decrease (-400) in MLAR disruptions.

The benchmark from 24/25 is 5,323, which translates to 1,331 disruptions per quarter. For Q2, disruptions are 15% (-404) below the benchmark target.

Home Office Target Not met

Response

In Q2 one region that had previously been a significant contributor to MLAR disruptions conducted some quality assurance work around their recording against all SOC threats in the region. This identified some areas where disruptions had been incorrectly applied and there was a re-issuing of guidance within some specific forces to prevent over recording.

This has resulted in a significant reduction this quarter and is likely to mean that over the whole reporting period disruptions are unlikely to increase given this significant change in recording processes.

This is a rectification of a previous recording issue and not a direct performance issue relating to MLAR disruptions.

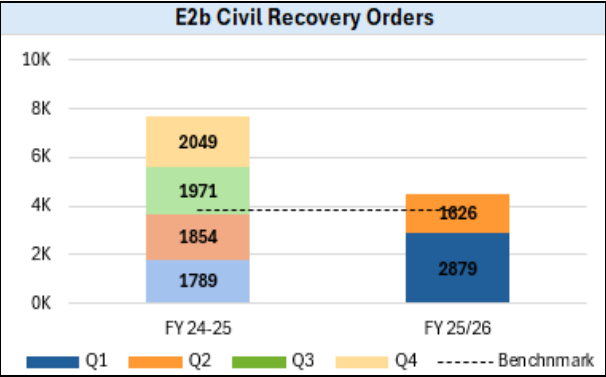
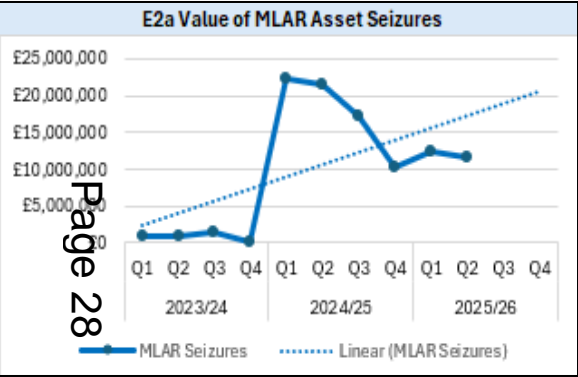
It is anticipated that this level will become the new normal activity level going forward.

We are expecting to see a rise in disruption activity in Q3 and Q4 as planned operations take place.

Performance Measure 2: We will seize and restrain more criminal assets through including released asset denial activity

Performance Measure 3: We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.

Success Measures:	FYTD Performance	Data Trend
E2a Increase the number of asset freezing orders, restrained assets, and recovered and confiscated assets.		↓
E2b Increase the number of Civil Recovery Orders.		⇒
E3 Recover a higher number of crypto assets.		↓



Analysis

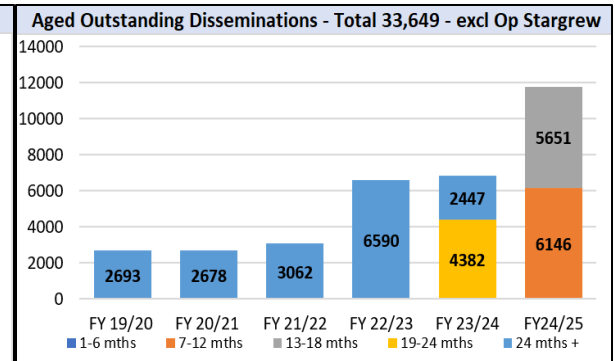
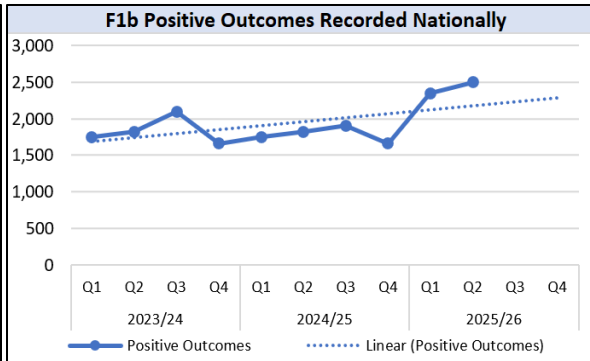
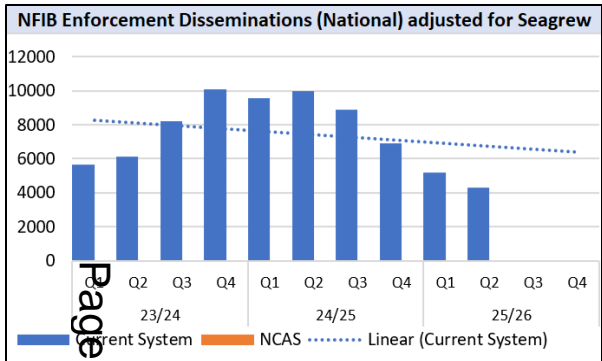
E2a In Q2 a value of £11,627,274 asset seizures was recorded for money laundering and asset recovery. In comparison to the previous quarter, this is a 7% decrease (-£849,192). In comparison to the same quarter for the previous year (Q2 24/25), this is a 46% decrease, however, Q1 & Q2 for 24/25 were extremely high quarters and outside of normal tolerance levels.

E2b Civil recovery figures in Q2 are reporting a 44% decrease (-1,253) in comparison to the previous quarter (Q1) and a 12% decrease (-228) in comparison to same period in 24/25 (Q2). Whilst the quarterly benchmark was not met, the level achieved was within normal variations and overall in FYTD we are maintaining an increased number of civil recovery orders.

E3 For Q2, there has been £81,751 in cryptocurrency seizures, this is 45% decrease (-£25,317) in comparison to the previous quarter and a 95% decrease in comparison to the same quarter for the previous year (Q2 24/25). The benchmarks for 24/25 is higher due to the significant seizures in Q1, Q2 remains below this benchmark and below normal seizure levels. There are currently only seizures recorded from one force/ROCU.

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages.

Success Measures:	FYTD Performance	Data Trend
F1a Increase the number of NFIB Pursue disseminations— Home Office Measure		⬇️
F1b Improve the positive outcome rate – Home Office Measure		⬆️
F1c Reduce the percentage of crime disseminations not yet assigned an outcome		➡️



F1a In Q2, NFIB disseminations decreased by 17% (-884) in comparison to Q1. In comparison to the same quarter for the previous year (Q2 24/25), disseminations have decreased by 57% (-5,678). Overall, disseminations are 46% below the 24/25 benchmark (-8,165). These figures are compared against dissemination data not including Op Stargrew which inflated the disseminations for Q1 24/25. The testing of the Foundry system has impacted business as usual, with reduction in performance likely to continue into the year as NFIB transition to the new service. **Home Office Target Not Met.**

F1b Nationally, there have been 2,499 positive outcomes during this period and 9,695 no further action outcomes. Overall, there is a 20% positive outcome rate. This is a 2% increase on Q1 24/25, with a positive outcome rate of 18% and a 37% increase in positive outcomes in comparison to the same period for the previous year (Q2 24/25). The Home Office quarterly target of 1,547 has been exceeded by 38% (952). **Home Office Target Exceeded.**

F1c In Q2, **33,649** NFIB disseminations from 19/20 to 24/25 had not been matched to an outcome. This is an increase of 6% (+1,808) from Q2 24/25 and decrease of 10% (-3,771) from the previous quarter, following the usual seasonal pattern. As in F1a, Op Stargrew disseminations have been excluded. A large proportion of these are with a single force and engagement attempts continue to try and reduce this. The next stage of this work is to identify a benchmark for what is a normal proportion of disseminations to be in ongoing investigations.

Response

NFIB

Testing of the new system is impacting usual capability. This is set to increase in Q3 due to training sections of the Crime Team ahead of go live. Performance is then expected to improve once staff are trained and working on the new platform. An increase in reporting has been observed, narrowing the known reporting gap.

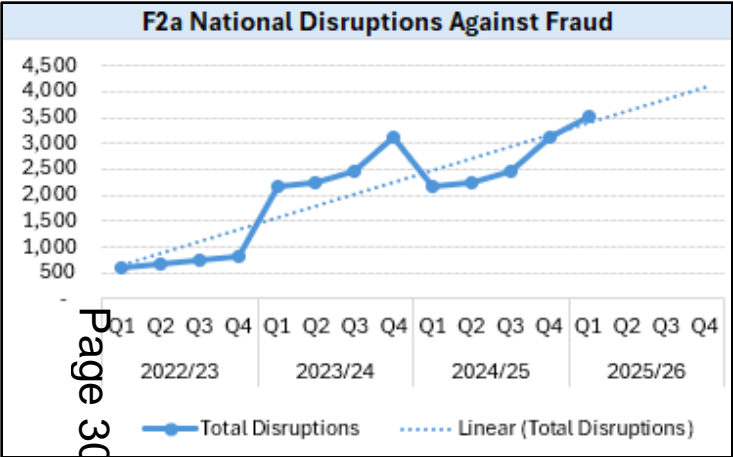
Outcomes

Key performance drivers across the first 6-month period include an Investment Fraud operation from CoLP yielding 1,199 outcomes in September. This is key to the Q2 performance as average monthly returns were beginning to drop, from 780 in Q1 to just 441 in Q2.

Q1 reflected strong monthly returns from many forces, in combination with large returns from two forces. These totalled more than 350 outcomes from each force in one month. It is these large one-off yields from forces that can push national annual positive outcomes from circa 6k to 8k per annum and even above the 24/25 total of 7,966 positive judicial outcomes.

Performance Measure 2: We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:	FYTD Performance	Data Trend
F2a Increase the number of disruptions against Fraud – Home Office Measure		↑



F2a Nationally, there were 3,515 disruptions recorded for Q1. This is a 62% increase in comparison to the same period for the previous year and 40% (+2,503) above the quarterly benchmark for 25/26.

- For fraud related disruptions there were:
- 33 major disruptions - 43% increase (+10) in comparison to Q1 24/25. Offender disruption accounted for 65% (26) of major disruptions, this includes actives such as arrests, convictions, warrants/searches.
 - 173 moderate disruptions - 12% increase (+18) in comparison to Q1 24/25. Offender disruption was also the highest activity for moderate disruptions at 42% (115).
 - 3,309 minor disruptions - 66% increase (+1,316) in comparison to Q1 24/25.

Across these disruptions 9 major disruptions related to OCGs or Priority Individuals(our most prolific offenders that are not linked to a specific group) and will have a significant impact. With a further 32 moderate disruptions relating to OCGs or Priority individuals.

Overall Specialist advice is the highest disruption type at 32% (1,417), followed by adult safeguarding at 21% (940). Specialist advice could involve many forms of targeted support or intervention such as educational or behavioural programs. Adult safeguarding involves a referral to the appropriate experts who can support the individual's needs such as social care, health professionals and or legal advice.

Home Office Target Exceeded

Response

There has been an increasing trend in positive outcomes over the past 2 years which correlates both to the change in criteria within the National Fraud Intelligence Bureau to determine which crimes are sent to forces to investigate with a greater focus on how solvable cases are, as well as greater embedding of the Fraud Investigation Model across forces and regions to increase the effectiveness of complex investigations by utilising disruptions more.

The aforementioned quality assurance work around the recording of disruptions against all SOC threats in a specific region has also impacted Fraud disruptions this quarter. However, it is less notable for fraud disruptions.

To ensure consistency the National Coordinators Office are working to produce some additional guidance with specific examples of good disruption recordings and inappropriate uses for fraud specific disruptions. This work is due to be circulated during Q3 and may result in a future reduction in recording as we grow data quality and remove those inappropriate recording practices that may currently exist.

Performance Measure 3: We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.

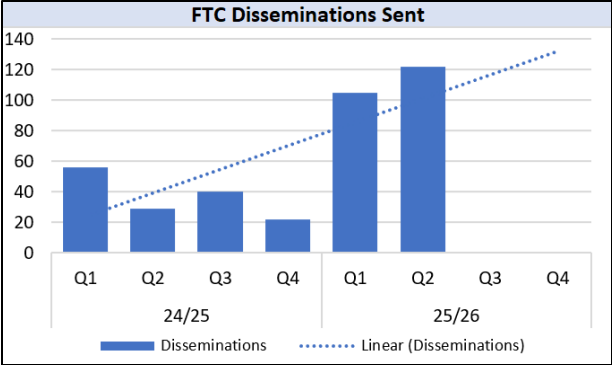
Performance Measure 4: We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations

Success Measures:	FYTD Performance	Data Trend
F3 Engage in all intensification efforts and target led national operations and evaluate operation-specific outcomes – Home Office Measure		⇒
F4 Increase the number of Fraud Targeting Cell (FTC) packages allocated, adopted, and investigated – Home Office Measure		↑

F3 In Q2, **Op Serrano** took place, this was a targeted intensification working alongside the Metropolitan Police in Hatton Garden. The operation targeted courier fraud which is a form of deception in which offenders impersonate trusted authorities to manipulate victims into handing over valuable items to a courier. This operation resulted in 13 arrests, eight charged, 63 proactive deployments and over £250,000 in cash seized. The intensification also created increased engagement with the Hatton Garden business community to raise awareness for a crime type that was noted to have cost previous victims over £21 million in the past financial year.

The NFFB’s investment fraud problem profile outlines the intelligence picture to inform law enforcement and partners, as well as helping direct PROTECT messaging. There is ongoing analytical work to monitor the investment fraud landscape and how it is evolving. **Op Hachi** has run from April 2025 and continued until August 2025. This international cross-organisational operation, led by INTERPOL, seeks to return money sent to overseas accounts that was generated by fraud (including Payment Diversion Fraud as well as other fraud types) and in previous years, has seen hundreds of thousands of funds returned to victims.

Home Office Target Met



F4 In Q2 a total of 122 disseminations were sent by the Fraud Targeting Cell (FTC). This was up 321% (+93) compared to Q2 of 24/25 and 16% (+17) from Q1 one of this year. The main driver for this was continuing work from Q1’s payment diversion fraud (PDF) Op Barton. FTC are currently working with ERSOU to develop intelligence obtained from Op Barton relating to OCGs engaged in money laundering and PDF.

There was progression on Op Seraphim; the development of Telegram channels advertising the sale of Fraud Enabling Products believed to be impacting the UK. Bulk subscriber applications are being submitted following initial checks and as results come back, intelligence packages will be produced and shared with Nigerian Police.

Response

Intensifications

In Q2 preparations for Operation Callback 2 have taken place. This operation aims to identify and arrest subjects involved in courier fraud. The MPS are leading the operation, and the London PECT will be staffing it and taking offences UK-wide. The objective is a reduction in the number of courier fraud offences, and the arrest and prosecution of offenders. Success will be measured by looking at offending patterns over time and measuring the number of arrests, charges and prosecutions. The operation will run for 8 weeks from 6th Oct to 30th Nov.

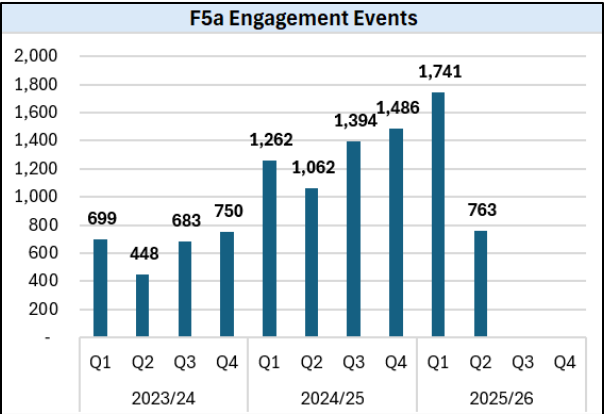
FTC

FTC have started a project around proactive identification of Investment Fraud at early stages, through a series of red flags and key indicators which was developed as part of the work on an operation last year. The intention is to identify Pursue opportunities for Fraud Ops as well as other early stages of disruption and intervention which should result in less victims becoming part of these schemes. Fraud Ops have continued to adopt cases developed by FTC. Discussions are ongoing with potential sources to feed in intelligence from early identification.

New SIM Farm Approach - Joint working between FTC, NCA FIT and CoLP has resulted in the attribution of six UK based handsets believed to be orchestrating bulk scam messaging campaigns impacting the UK. Executive action is planned for November.

Performance Measure 5: We will develop and deliver a centrally co-ordinated National Fraud PROTECT Network that will align with the National Cyber PROTECT Network, share best practice, and promote local delivery of national messaging.

Success Measures:	FYTD Performance	Data Trend
F5a Increase the number of Protect engagement events and attendees – Home Office Measure		↓
F5b Percentage of protect engagement event attendees satisfied with the engagement they attended – Home Office Measure		⇒
F5c Percentage of protect engagement event attendees likely to change their behaviours as a result of engagement – Home Office Measure		⇒



F5a For Q2, **763 engagements** were held across the network, with **38,867 attendees**. Q2 is reporting a 56% (-1,111) decrease in comparison to the previous quarter and a 28%(298) decrease on Q2 24/25. Phase 2 of project Aegis is now complete, and the results are being analysed by the London School of Economics. **Home Office Target Not Met**

F5b&c The fraud protect surveys continue to be adopted by the national Fraud Protect Network during their presentations, events and interactions with citizens and businesses across the country. In FQ2 **98%** were very satisfied and satisfied with the event/engagement (no change from Q1) **99%** were likely to change their behaviour or already undertake that behaviour (1% increase from Q1). **Home Office Target Met**

In Response

During Q2 a review of how fraud protect work was being carried out was undertaken. This is leading to a more focussed effort in the protect engagement and tactics to be undertaken. It is therefore likely that this will lead to lower volumes of engagement events in future quarters, but with a greater impact of the advice received.

This was, in part, informed by the work of Project Aegis which took place this quarter in collaboration with the Home Office and London School of Economics. It focussed on specific Protect advice measures provided to those who they consider are at risk of Online Shopping Fraud or Investment Fraud, to determine the most effective methods in this area. Full analysis and findings are being undertaken and will be shared – this behaviour change learning is crucial to the protect strategy that is also in development.

To ensure the impact of wider protect campaigns can also be measured, work to develop a tool for greater understanding of behaviour change linked to social media posts and engagement is also underway in Q3.

This more directed approach in Q3 will focus on

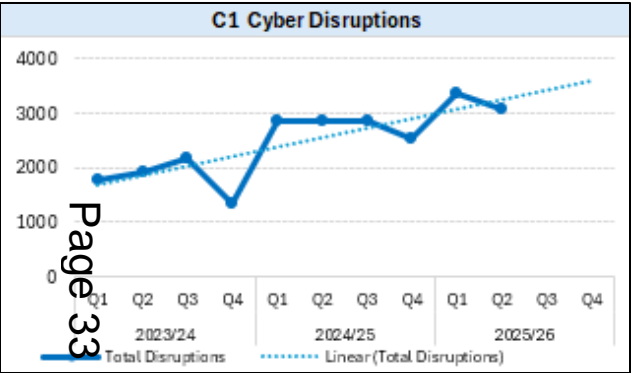
- Working with students to raise awareness of frauds targeting them as they start or return to university.
- Fraud Protect & Cyber Security in Social Care designed specifically for professionals working in the social care sector.
- Online shopping fraud focus.

The network will be partnering with Barclays during November, collaborating on delivering a consistent national protect message with protect officers and Barclays staff. This will also utilise Barclays ‘scam vans’ in 40 retail locations throughout the UK delivering consistent protect advice to the public ahead of Black Friday and the festive period where online shopping itself peaks.

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.

Performance Measure 2: We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.

Success Measures:	FYTD Performance	Data Trend
C1 Increase the number of disruptions against cyber crime		⇒
C2 Increase the number of operations involving the Computer Misuse Act (CMA)		↑



C1. In Q2, there were a total of 3,082 disruptions.

- 1 major disruptions - 75% decrease (-3) in comparison to Q1 25/26
- 66 moderate disruptions - 1% decrease (-1) in comparison to Q1 25/26
- 3,015 minor disruptions - 9% decrease (-288) in comparison to Q1 25/26.

The top 2 disruption types are specialist advice at 79% (2,436) and safeguarding at 11% (330).

In comparison to the previous quarter (Q1), Cyber disruptions are reporting a 9% decrease (-292). In comparison to the same quarter for the previous year (Q2 24/25), there has been an 8% increase (+221).

The benchmark from 24/25 is 11,085, which translates to 2,771 disruptions per quarter. For the FYTD Q2, disruptions are 16% (+914) above the benchmark.

Response

During 24/25 the South East Region, who were piloting the regional control model, accounted for 30% of major and 12% of moderate pursue disruptions across the cyber network. Over Q1 & Q2 in 25/26 the South East region has experienced significant resource challenges which has impacted operational activity. Partly as a result, no major and a reduced number of moderate disruptions have been recorded in the South East. Overall, quarterly fluctuations are expected in the delivery of major and moderate disruptions.

The NPCC Serious and Organised Crime portfolio is currently undertaking an APMIS consistency review across all SOC (including fraud and cyber) recorded disruptions. The team identified that regions and forces are regularly recording effort rather than impact, some regions (as mentioned in other areas of this report) have already taken proactive action to change this, which has impacted disruption recording numbers.

Through raising awareness and educating those inputting disruptions on the need to focus on impact, the consistency review will undoubtedly result in reductions in disruption volumes, however, will improve the overall quality of the information being used.

C2. For Q2, there have been a total of 1,737 Vulnerability Notification Packs and Malicious Notification Packs (that informs an organisation about potential weakness in its systems or an alert of malicious behaviour detected on the network such as attempted intrusions) distributed to national and regional Cyber Crime Units. The number of Malicious Notification packs distributed across the cyber network has risen **76%** since Q1 25/26, whilst the vulnerability packs have increased by **123%**.

Under the title **Project Capstone**, the NPCC Cybercrime Team continues to progress its partnership working with several private sector partners, developing intelligence opportunities to identify UK based cyber criminals and those utilising cyber enabled tools and cryptocurrencies in furtherance of their criminal activities. Q2 25/26 has seen 22 additional intelligence packages disseminated to the ROCU network.

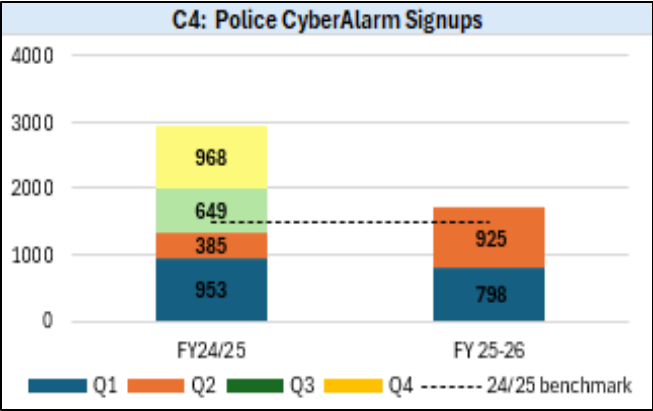
Performance Measure 3: We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.

Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations they engage with.

Success Measures:	FYTD Performance	Data Trend
C3 Increase PROTECT notifications issued to victim organisations.		⇌
C4 Protect Officers to promote Police CyberAlarm to SME organisations.		⇌

C3 A Protect Notification is a method used to notify victim organisations when intelligence is received indicating a cyber crime has occurred or is likely to occur against their IT system. If the intelligence suggests a live cyber security threat where quick time actions are needed, then it will be treated as urgent and TICAT will deliver the notification via phone, or via the Protect Network for a same day in-person visit to the premises.

During Q2, the network reports 83 disseminations, of which 76 (91%) were completed within the Quarter. This is similar to Q1 24/25 where 93% (75) of the 80 notifications were completed within the quarter. Protect Notification outcomes are captured, helping to improve the recording of cybercrime in the UK and quantify the impact of the Protect network; 35% of the Q1&Q2 25/26 taskings have confirmed incidents and crime reports raised.



C4 In Q2 25/26, 925 Small to Medium-sized enterprises (SMEs) signed up to Police CyberAlarm. This is a 16% increase (+127) in comparison to Q1 and 140% increase (+540) in comparison to the same period for the previous year (Q2 24/25). Overall, performance is reporting 17% above the 24/25 benchmark (+245).

Member Sign-ups increased so far this year 25/26 due to an increased push from the Department for Education for schools to register as part of the Risk Protection Agreement. Growth was quieter during August 2025 as expected as the schools closed for the summer period.

Response
Protect Notifications
The Cyber Protect network is seeking to pivot towards intelligence-led interventions, primarily through Protect Notifications. By directly targeting businesses where intelligence indicates a cyber crime has occurred or is likely to occur against their IT system, a Protect intervention can also prevent multiple onward crimes perpetrated through their systems.

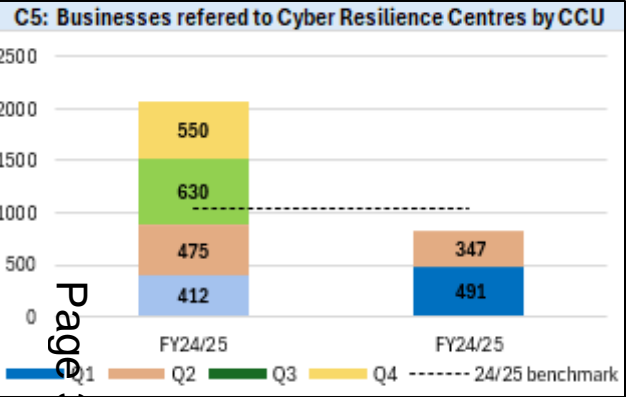
To enable this, NPCC Cyber are working with the NCCU on its Proactive Protect Project, whereby data from NCSC Early Warning System and PCA intelligence is pooled. This will lead to an increase in the volumes of Protect Notifications and targeted Protect interventions, and we aim to continue to meet the high levels of performance seen quarter on quarter despite increasing demands.

PCA
Police CyberAlarm (PCA) is undertaking a procurement exercise, which will result in a new provider. Subsequently, the PCA focus is on delivering a seamless transition, which is likely to negatively impact the drive to increase member sign-ups as capacity is reduced to facilitate this transition work.

However, in August 2025, PCA changed the registration process to make it quicker and easier with automated approvals and fewer registrations details required, which is likely to increase the number of sign-ups. Furthermore, PCA have commenced the use of a marketing company, with the aim to increase growth later within the reporting year.

Performance Measure 5: We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other’s work and grow CRC membership

Success Measures:	FYTD Performance	Data Trend
C5 Increase the number of Cyber Crime Unit referrals to Cyber Resilience Centres		↓



C5

In Q2, the number of Cyber Resilience Centre (CRC) referrals decreased by 29% (-144) in comparison to the previous quarter.

Referrals have also decreased by 27% (128), in comparison to the same quarter for the previous year (Q2 Q4/25). Overall, figures are reporting 38% (195), under the benchmark for this FYTD.

Response

Of note the Protect network has delivered 8% fewer engagement events during April and May compared to the same period in 24/25, due to staffing vacancies across the networks from funding uncertainty. This is the main pathway for businesses to be referred to cyber resilience centres and there is a significant dependency between engagement events and CRC referrals. These funding concerns were alleviated in June 2025, however there will have been a continuing impact in Q2 from the lower levels of engagement activity.

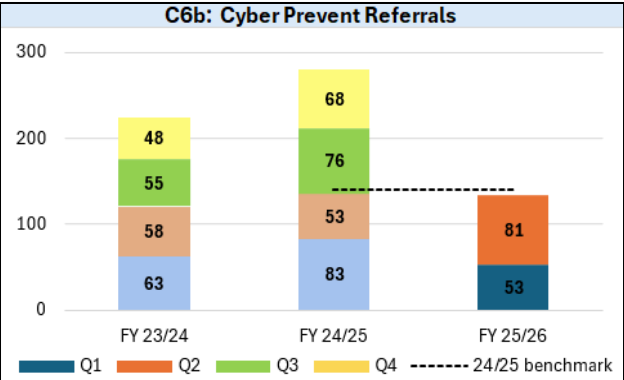
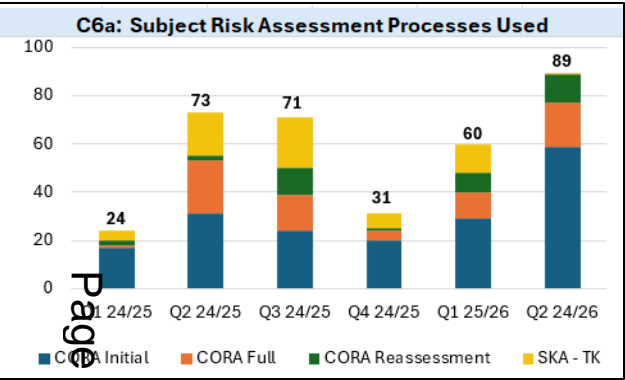
The CRCs are currently transitioning into a new police structure and closing as businesses. This will be completed by December 2025. Regional CRCs will be wound up as limited companies and fall within Policing (staff will be seconded to CoLP). This will ensure greater professionalism and consistency of delivery.

The National Cyber Resilience Centre Group will provide high quality, consistent marketing and branding as well as oversee delivery of all student CyberPath services for all CRCs .

The new CRC Strategy and Delivery Plan will focus on membership growth, Cyber Path delivery and Cyber Essentials.

Performance Measure 6: We will develop improved referral process for new nominals - to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.

FYTD	FYTD Performance	Data Trend
C6a Increase the number of CORA assessments made		⬆
C6b Increase the number of PREVENT referrals		⬆



Response

The number of individuals identified is based on information coming in to teams from schools, parents, investigations, etc. Following this intelligence development is required by Cyber Prevent staff to turn these in to formal Cyber Prevent referrals.

The number of referrals is therefore directly linked to the capacity within cyber prevent teams. These teams have been reduced due to reprioritisation by the Home Office and funding therefore subsequently reduced in 25/26.

As such it is unlikely that the number of referrals is going to increase in 25/26 however the ambition to maintain the number of referrals from 2204/25 is now being worked to achieve.

C6a A CORA assessment is used to assess the risk posed by individuals referred and helps determine the level of cyber capability from skills, knowledge, and access to technology. This helps decision making in deciding the appropriate intervention, diversion, or support to proceed with. For Q2, risk assessments have increased by 49% in comparison to Q1 and by 22% (+16) compared to the same period for the previous year (Q2 24/25).

A key focus for CORA in 25/26 is the completion of an assessment at the end of an individual’s participation in the Cyber Choices Programme. This will allow the impact of interventions to be measured, highlighting those that are most effective in reducing risk, it is positive that these reassessments continue to increase quarter on quarter.

C6b A total of 81 Cyber Prevent referrals were received in Q2, a 53% (+28) increase from Q1 and a 1% decrease (-2) from the same period for the previous year (Q2 24/25). Halfway through the performance year, 25/26 referrals sit at 48% of total 24/25 returns.

The first academic study into recidivist rates following Cyber Choices intervention(s) is underway. The study will provide a critical understanding of the impact of cyber prevent interventions.

Counter Terrorism and Home Office Prevent have delivered guidance on the relationship between cyber policing, NCA, and CT Prevent who all work to achieve similar aims in their fields. This builds on a North East regional pilot and aims to formalise existing processes, ensuring Counter Terrorism and Cyber risks are appropriately managed, documented, owned and relationships clear. This is especially important as Counter Terrorism Prevent remains the network’s second-largest source of referrals after schools.

The first revamped Prevent Managers’ Governance Meeting took place in September 25. with representatives from NPCC, NCCU Prevent, and the Home Office. The focus of the meeting is on performance and best practice, and we will report on identified learnings form that forum as it progresses.

Performance Measure 7: We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.

FYTD	FYTD Performance	Data Trend
C7 Increase the number of CDSV Programme participants and their utilization across the network.		↑

C7 In Q2, **4 new volunteers** joined the network during Q2, across three different force/regional teams, bringing the total to **144 in 35 teams**.

In Q2, CDSVs logged activity across all four Ps, a summary of some of the activity:

- Development of national automated protect notification outcome form.
- Supporting development of the new CRC survey.
- Various Fraud and Cyber Protect Engagements
- Dark net monitoring and research
- Converting apps and games into Welsh
- Developing interactive apps/engagement tools
- Assisting with Hydra cyber exercise

Recruitment also commenced for new and existing volunteers to become part of the new Specialist Crime Volunteer Network National Co-ordination Team, to provide their expert strategic advice and different perspectives.

The Office of the Police Chief Scientific Adviser released their report; Developing a Science and Technology Profession for Policing: Building an Evidence Base, as stage one in their three-year strategy to establish a dedicated Science and Technology (S&T) profession within policing, to navigate the rapidly evolving landscape driven by advancements in S&T. Expansion of the use of Specialist Crime Volunteers and the national platform (Assemble) were a key recommendation in the report.

Response

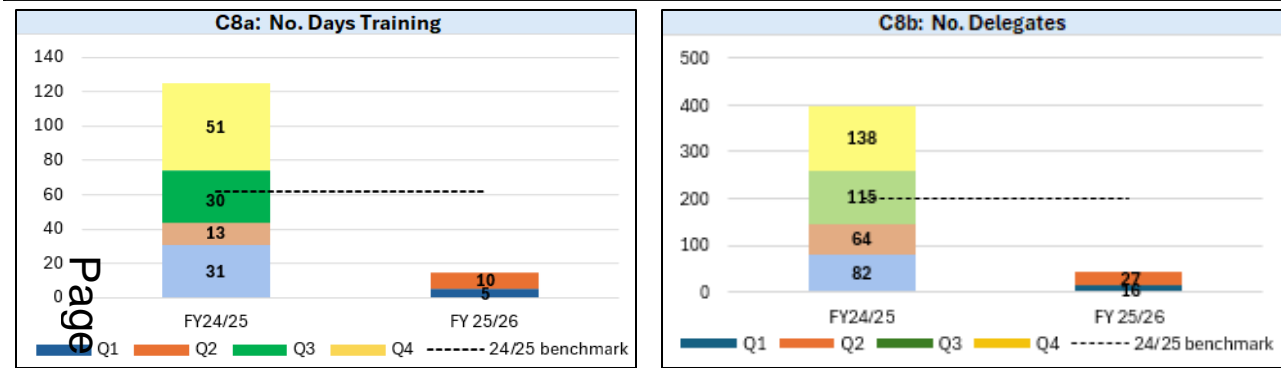
Grant funding from the Cyber Policy Unit has been doubled, allowing for the recruitment of 2 full-time roles to progress recommendations from the 2024/25 academic review, deliver a new strategy and partner with key organisations to facilitate focused recruitment.

Successful candidates were selected in July/August and are awaiting start dates.

CDSV will be rebranded to become the Specialist Crime Volunteer Network (SCVN) and will encompass not only cyber but support to the wider economic crime portfolio. This wider support and growth will be a key priority for the new team when they start.

Performance Measure 8: We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.

Success Measures:	FYTD Performance	Data Trend
C8a Increase the number of Cyber training days		↓
C8b Increase the number of Cyber training delegates		↓



Response

Due to a delay in the 25/26 Home Office grant confirmation the extension of the current training contract was delayed meaning a gap in delivery as there was no contract in place for delivery of training. The extension is now in place with new courses planned over the year now summer is over where seasonally training attendance across all of policing is low. It is anticipated there will be an increase in training delegates and days delivered in Q3.

A demand analysis of the cyber network was completed in Q4 24/25 to provide an understanding of the courses required during 25/26 this looked at the number of staff across the network still requiring training. This number is lessening due to the levels of training that have been provided to date and there is now a focus on CPD for those that have already received the initial training.

In addition to formal training captured in C8a and C8b is the provision of continuous professional development through the gamified learning system delivered by the SudoCyber collaboration. This allows staff to continue learning at their own pace and understand how to tactically respond to emerging threats. There was a 40% increase in training labs completed in Q2 25/26 when compared against Q1 25/26, this followed the promotion of a Capture The Flag (CTF) competition which started on 22 September 25. There are currently 102 registered users, with the top 3 scorers in each regions being invited to a final on 25th November 25.

The CTF is designed to raise awareness and usage of the SudoCyber online training platform; an alternative means of professional development via its online training portal.

Additionally following the success of a pilot, a further Cyber Incident Management course, designed to develop Senior Investigating Officers understanding of how law enforcement responds and supports the victim of a reported cybercrime is set to run Q3 25/26. This is a notable training gap for senior leaders within policing that is now being addressed.

C8a During Q2, 27 delegates were delivered formal training courses, this is a 69% increase (+11) in comparison to Q1 and a 58% decrease (-37) when compared to the same period for the previous year (Q2 24/25). Overall, Q2 is reporting 79% under the benchmark (-157).

C8b For Q2, there has been a 100% increase (+5) in the number of formal training days provided in comparison to Q1. In comparison to the same quarter for the previous year (Q2 24/25), there has been a 23% decrease (-3). Q2 is reporting 76% below the benchmark (-47).

SudoCyber	Labs Completed
Jul-25	417
Aug-25	248
Sep-25	634
Total	1,299

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee (ECCC)	Dated: 4 November 2025
Subject: Summary of Action Fraud public complaints data – Q2 2025/26	Public report: For Information
This proposal: <ul style="list-style-type: none"> Provides statutory duties 	Public trust and confidence
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	N/A
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Commissioner of the City of London Police
Report author:	Detective Superintendent Carly Humphreys

Summary

The attached quarterly report produced by the Professional Standards Department provides members with an overview regarding Action Fraud complaints.

In Q2 2025/26, a total of 131 Schedule 3 complaints were logged, doubling from Q1 (100% increase), and exceeding the five-quarter average of 114. However, discrepancies were found between complaints logged in AF SUGAR and the PSD Centurion database, which are being addressed. Non-Schedule 3 complaints rose by 20% to 125, while allegations increased by 11% to 131, slightly above the five-quarter average of 124. The most common allegation category was "Police action following contact" (76), followed by "General level of service" (36) and "Information" (13), largely driven by unmet expectations regarding Action Fraud investigations.

Complaint finalisations also rose significantly: Schedule 3 finalisations increased by 170% (27 cases), contributing to a total of 96 cases finalised in Q2—33% more than

Q1 and above the five-quarter average of 88. Non-Schedule 3 finalisations rose by 11%. Timeliness data for logging and contacting complainants was unavailable for Q2. The average time to finalise Schedule 3 complaints was 202 days, and 175 days for non-Schedule 3, based on retrospective IOPC bulletins.

Additional insights include a rise in MP-related cases (105, up from 63 in Q1), and Action Fraud reporting increased across all categories: 147,394 total reports (10% rise), 113,613 crime reports (13% rise), and 48,300 information reports (4% rise). Despite this, complaints represented only 0.09% of total Action Fraud reports. Satisfaction survey engagement remained low, with only 1.6% of recipients opening the survey and 1.3% providing feedback.

Recommendation(s)

Members are asked to:

Note the report.

Appendices

- Appendix 1 – Summary of Action Fraud public complaints data– Q2 2025/26

Carly Humphreys

Detective Superintendent Carly Humphreys
Head of Professional Standards

T: 07523 946343

E: carly.humphreys@cityoflondon.police.uk

Summary of Action Fraud public complaints data– Q2 2025/26				
Metric	Current quarter (Q2)	Previous quarter (Q1)	(%) change (Q on Q)	Comment
Complaints – Schedule 3	6	3	100%	<p>A total of 131 cases were logged in Q2 2025/26. This is an overall increase of 24 cases from Q1 2025/26 (22%)</p> <p>The average number of cases logged over the previous 5 quarters is 114 per quarter, Q2 is above average.</p> <p>It has been identified not all complaints logged in the AF SUGAR system have been logged into the PSD (centurion database). This is being rectified¹.</p>
Complaints – not Schedule 3	125	104	20%	
Allegations	131	118	11%	
Average time to log complaints (days)	N/K	6	-	<p>There were 131 allegations recorded in Q2 2025/26. This is an increase of 13 allegations from Q1 2025/26 (11%).</p> <p>The average number of allegations over the previous 5 quarters is 124 per quarter. Q2 is just above average.</p> <p><i>Timeliness is taken from IOPC published bulletins and available retrospectively, unavailable dataset from Centurion.</i></p>
Average time to contact complainant (days)	N/K	2	-	
Complaints finalised – Schedule 3	27	10	170%	<p>A total of 96 cases were finalised in Q2 2025/26. This is an overall increase of 24 cases from Q1 2025/26 (33%)</p> <p>Average number of total cases finalised is 88 over the last 5 quarters. Q2 is therefore above average.</p>
Complaints finalised - not Schedule 3	69	62	11%	
Average time to finalise complaint cases (days) – Schedule 3	202 average combined data	241	n/a	<p><i>Timeliness is taken from IOPC published bulletins and available retrospectively.</i></p> <p><i>Quarter Case combined data average 202 days (ex subjudice) from Centurion.</i></p> <p><i>IOPC bulletin will publish breakdown by case type logged (YTD – Q1 therefore average of the yearly data)</i></p>
Average time to finalise complaint cases (days) – not Schedule 3		175	n/a	
Applications for review sent to local policing body (appeals)	1	1	0	One recorded during Q1 – Not valid as did not meet criteria
Applications for review sent to IOPC (appeals)	0	1	0	None recorded during Q2

Nature of allegations – Of the 131 allegations recorded during Q2 2025/26 the highest number was in the category of, A1 – Police action following contact (76) followed by General level of Service (36) and A3 – Information (13). Reasons for complaint mostly relate to customer expectation of Action Fraud, with either the lack of contact or investigation cited. This is an increase in allegations recorded against Q1 of 13 (11%).

Members of Parliament –

There have been 105 miscellaneous cases logged where MPs have contacted PSD on behalf of a constituent. This is an increase of 42 against the previous quarter. The average being logged as 64 over the last 5 quarters.

Action Fraud –

In **QTR 2** of the 2025/26 Financial Year Action Fraud recorded **147,394** reports on the National Fraud Database (Increase 10% v QTR 1)

In **QTR 2** of the 2025/26 Financial Year Action Fraud recorded **113,613** crime reports (Increase 13% v QTR 1), and **48,300** Information reports (Increase 4% v QTR 1)

Action Fraud delivered the confirmation survey hyperlink to all victims who reported a crime via the Contact Centre voice channel or via the web reporting tool.

(Source: Sugar CRM (raw, uncleaned data extracted at date of publication, including bulk reports)

1,824 (1.6%) of the **113,613** ‘confirmation’ survey hyperlinks delivered to victims were opened in **QTR 2** with **1,427** (1.3%) of recipients opting to provide satisfaction feedback.

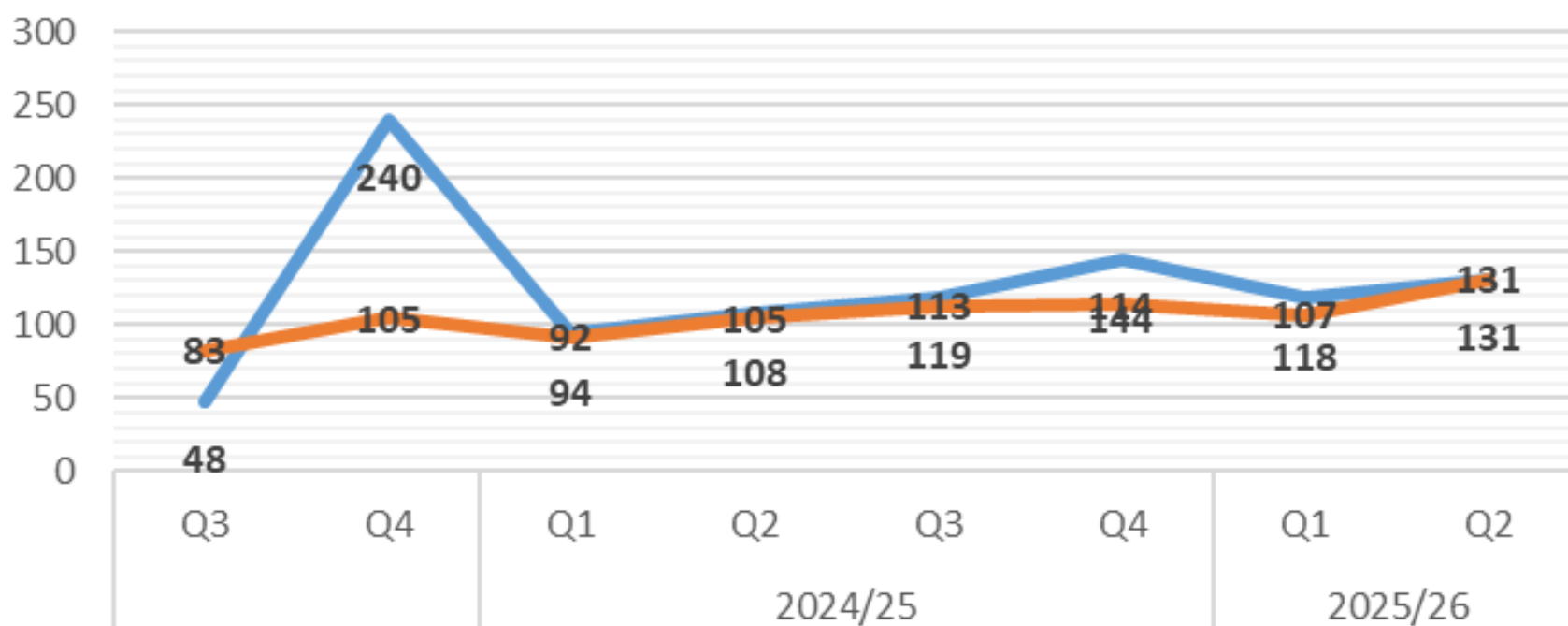
The complaint figures (total) represent 0.09% of the total number of Action Fraud reports recorded in Q2.

¹ All dissatisfaction data should be logged on Centurion (PSD) to reflect true public complaint data relating to Action Fraud. This is essentially a manual process from Sugar (the customer facing Action Fraud website) and inputted to Centurion. There are issues with Sugar, as the website allows complaints to be made, the identification of what might be defined as a complaint (as some of these are not complaints), and then referring identified complaints to PSD. In order to rectify this issue. 1. We are manually capturing and transferring AF Sugar complaints to PSD and 2. There is PSD engagement with the facilitation of the new AF/NFIB systems (however, there are no plans to automate the ‘complaints’ into Centurion at this time).

--	--

Action Fraud complaint data

— Total Action Fraud Allegations recorded
— Total Action Fraud Complaints logged



City of London Corporation Committee Report

Committee(s): Economic and Cyber Crime Committee	Dated: 04/11/2025
Subject: Cyber Griffin Update	Public report: For information
This proposal: <ul style="list-style-type: none"> • delivers Corporate Plan 2024-29 outcomes • provides statutory duties • provides business enabling functions 	CoLP impact the following Corp Plan outcomes: Vibrant Thriving Destination- (Community Safety/ CT) Dynamic Economic Growth- (National Lead Force)
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£-
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	The Commissioner
Report author:	Charlie Morrison, Helen Thurtlesmith

Summary

Cyber Griffin remains no track to achieve the highest performing year to date. The programme has continued to develop new services which close gaps in the current service offering and have begun assessing service impact using a new longitudinal qualitative assessment model.

Recommendation(s)

- Note the report

Main Report

Background

This report gives a brief update on the current position of Cyber Griffin. The programme currently offers 6 core services: Baseline Briefing, Table Top Exercise, Cyber Capability Assessment, Incident Response Training, Case Study: Spear Phishing, and the Incident Response Hydra.

For further details of all services please visit: www.cybergriffin.police.uk

Current Position

1. In Q2/2025, Cyber Griffin trained 5,880 delegates which was 130% of the quarter's target of 4,500. Conducted 154 services, which was 154% of target, and partnered with 84 new businesses, 168% of target, see *Figures 1,2,3*.

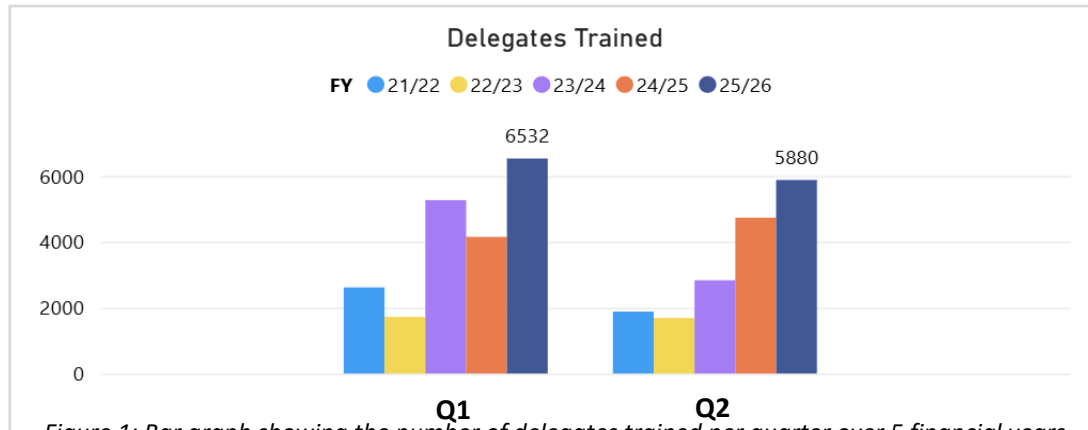


Figure 1: Bar graph showing the number of delegates trained per quarter over 5 financial years

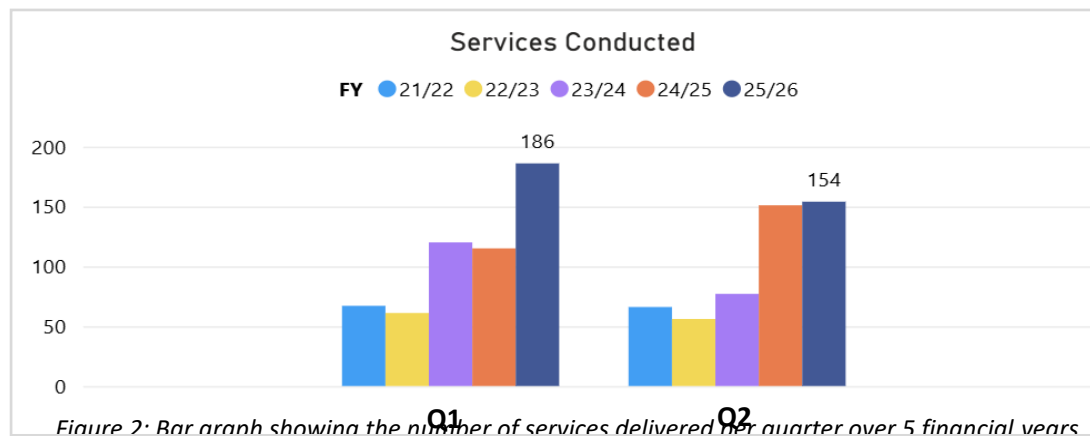


Figure 2: Bar graph showing the number of services delivered per quarter over 5 financial years

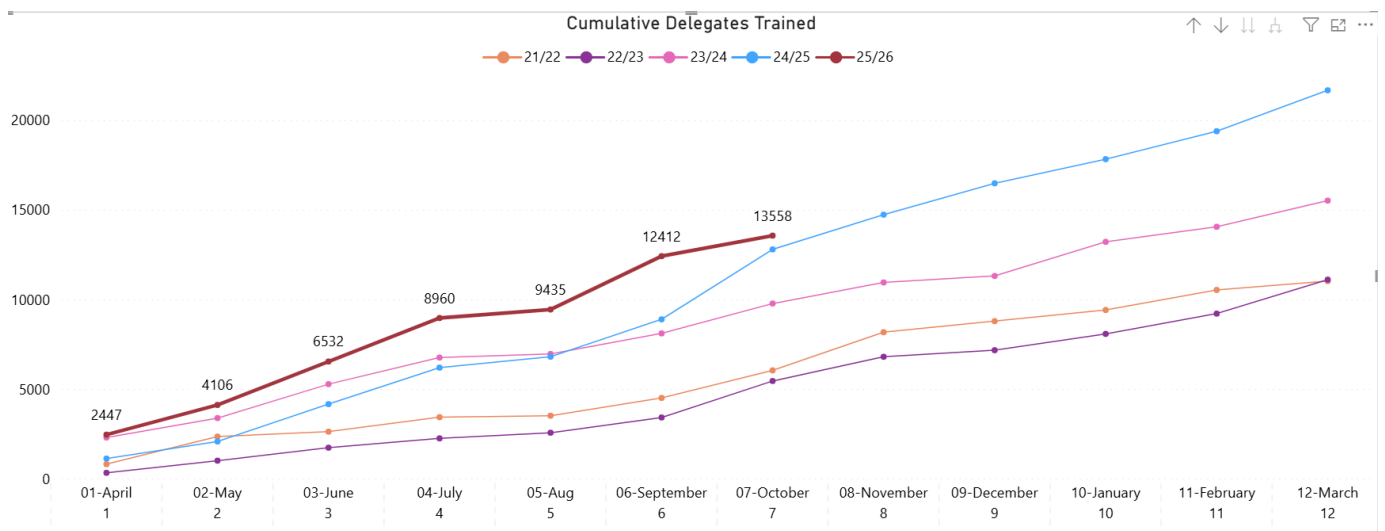


Figure 3: Line graph showing the number of delegates trained (cumulative) over 5 financial years

2. Regarding performance against national targets, Cyber Griffin continues to meet all nationally set key performance indicators (KPIs). Specifically, the programme has engaged with 100% of victims of cyber-dependent crime. Survey data also demonstrates that engagements create security behaviour changes in above 75% of delegates. The same events have a satisfaction rate of considerably above 75%.
3. The programme's development of a new service aimed at supporting parents and guardians in the Square Mile has progressed. This briefing is currently in beta testing and has been delivered to over 1,200 delegates. CPD® accreditation has been applied for, and it is expected that this service will be available in the form of digital evening briefings from January 2026. Initial feedback remains extremely positive.
4. Cyber Griffin has created a process to assess the impact of its work and begun to collect data. The initial findings are very positive however the sample size is not yet large enough to infer significant findings. This work will be further reported on as stable finding emerge.
5. Cyber Griffin have completed its revisions of the Baseline Briefing, the programme's security awareness presentations. The Baseline Briefing 6.0 is ready for launch and is fortunate to have the support of The Fishmongers' Company who have provided a venue. The briefing remains reflective of the latest threat landscape and NCSC advice.

6. The programme has retained funding from the Corporation Business Levy and the NPCC Cyber Crime Programme until March 2027. As funding streams are fixed, they do not consider year on year financial increases to salaries and professional fees. Cost reviews have been conducted internally, and a full report is due to be created. This report will be made available to the committee in the next performance return.

Conclusion

Cyber Griffin remains on course to achieve its highest performing year to date. The programmes' projected to deliver to 6% more delegates and 14% more services compared with the last financial year. The programme's focus remains on improving and assessing the impact of its offering using new assessment tools. Performance in Q3 is expected to be very high, given it includes Cyber Security Awareness

Report Authors:

Inspector Charlie Morrison

Head of Cyber Griffin, Cyber Crime Unit, Specialist Operations Directorate

E: Charlie.morrison@cityoflondon.police.uk

Helen Thurtlesmith

Project Manager

E: Helen.thurtlesmith@cityoflondon.police.uk

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

By virtue of paragraph(s) 3, 7 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank