Public Document Pack

CITY OF LONDON

Economic Security and Cyber Crime Committee

Date: **MONDAY, 23 FEBRUARY 2026**

Time: 11.00 am

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

Members:
Tijs Broeke, Chair (Chair)
Deputy Madush Gupta (Deputy Chair)
Melissa Collett
Alderman Professor Emma Edhem
Jason Groves
Naresh Hari Sonpar
Mandeep Thandi
Deputy James Thomson CBE
James Tumbridge
Deputy Dawn Wright
Kwaku Osafo

Enquiries: **Kezia Barrass**
Kezia.Barrass@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 4 November 2025.

For Decision
(Pages 5 - 10)

4. **PUBLIC OUTSTANDING ACTIONS**
Joint report of the Commissioner and the Town Clerk.

For Information
(Pages 11 - 12)

5. **DEPUTY COMMISSIONER'S UPDATE (NATIONAL LEADERSHIP FUNCTIONS)**
Report of the Commissioner.

For Information
(Pages 13 - 18)

6. **POLICING PLAN PERFORMANCE REPORT - Q3 2025/26**
Report of the Commissioner.

For Information
(Pages 19 - 54)

7. **NLF PERFORMANCE FRAMEWORK REFRESH**
Report of the Commissioner.

For Information
(Pages 55 - 58)

8. **SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA**
Report of the Commissioner.

For Information
(Pages 59 - 64)

9. **CYBER RESILIENCE CENTRE (CRC) NETWORK UPDATE**
Report of the Commissioner.

For Information
(Pages 65 - 80)

10. **INNOVATION & GROWTH - UPDATE OF CYBER & ECONOMIC CRIME RELATED ACTIVITIES**
Report of the Executive Director of Innovation and Growth

For Information
(Pages 81 - 84)

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

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

13. **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

14. **NON-PUBLIC MINUTES**
To agree the non-public minutes of the meeting held on 4 November 2025.

For Decision
(Pages 85 - 88)

15. **NON-PUBLIC OUTSTANDING ACTIONS**
Joint report of the Commissioner and the Town Clerk.

For Information
(Pages 89 - 90)

16. **DOMESTIC CORRUPTION UNIT 2026-2029**
Report of the Commissioner.

For Decision
(Pages 91 - 96)

17. **FCCRAS UPDATE**
Report of the Commissioner.

For Information
(Pages 97 - 110)

18. **REPORT FRAUD FULL LAUNCH PRESENTATION**
Report of the Commissioner.

For Information
(Pages 111 - 120)

19. **CITY OF LONDON POLICE ASSET MANAGEMENT OFFICE**
Report of the Commissioner.

For Information
(Pages 121 - 124)

20. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**
Joint report of the Town Clerk and the Commissioner.

For Information
(Pages 125 - 136)

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

22. **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
Tuesday, 4 November 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 Tuesday, 4 November 2025 at 11.00 am

Present

Members:
Tijs Broeke (Chair)
Deputy Madush Gupta (Deputy Chair)
Melissa Collett
Jason Groves
James Tumbridge
Deputy Dawn Wright

Officers:

Alex Orme	-	Town Clerk's Department
Oliver Bolton	-	Town Clerk's Department
Hayley Williams	-	Chief of Staff
Teresa La Thangue	-	Public Relations Office

1. **APOLOGIES**
Apologies were received from Naresh Sonpar, Deputy Chris Hayward and Deputy James Thomson.

2. **MEMBER'S 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 8 September 2025 be approved as an accurate record.

4. **POLICING PLAN PERFORMANCE REPORT – Q2 2025/26**
The Committee received a report of the Commissioner with an assessment of the 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 2 2025/26 (1 July 2025 – 30 September 2025). Officers advised that Q2 had been a good quarter both locally and nationally. In respect of local City performance, Members noted that technology disruptions continued to be down this quarter and age disseminations were on target.

At the national level, Officers advised that performance in Q2 has also been positive. Officers reported continued improvement across many performance measures, though some were nearing the end of their lifecycle. Members noted that cyber training and Protect were areas below target and suggested that a refreshment of performance framework measures be bought to the next committee meeting in 2026. Officers further advised that Protect activity reductions reflected maturing practice and a shift in strategy for victim protection, including increased focus on online and social-media-based engagement rather than face-to-face activity. Officers expected Protect engagement figures to continue to decrease as this pivot continued. Due to FCRASS and the imminent launch of Report Fraud, age dissemination performance within 28 days had reduced; however, Officers anticipated a strong position by Q4 as new technology bedded in.

On Cyber Resilience Centres (CRCs), Officers reported that the network was undergoing a period of change to be completed by the end of December, with improvements expected by Q4. Regarding money laundering and asset recovery (MLAR), Officers advised that the area was currently below target due to disruptions and system-related issues, including corrections to what could be counted.

Officers emphasised that they were not concerned by the underperforming areas, each having reasonable explanation, and indicated an intention to bring forward proposals for revised measures for the next 2.5 years.

A Member asked about improving outcomes for victims. Officers confirmed that performance was improving on current measures. Officers highlighted the contribution of the DCPCU, noting that £75m of potential fraud offences had been prevented this year compared with £53m last year. Officers added that Report Fraud would enable broader visibility of stop-and-block disruptions, including social-media takedowns.

A Member asked about training and whether a “train-the-trainer” model could be explored in the forthcoming report. Officers advised that a national lunch-and-learn series had been used to promote courses to Assistant Chief Constables and strategic leaders, including recent sessions on the fraud performance accelerator. Officers reported strong feedback, with a 9/10 value-for-time rating and 8/10 confidence rating.

A Member requested early sight of the broader Protect strategy and related training courses, suggesting that a high-level plan would be helpful.

A Member raised the need for a national approach connecting frontline policing, specialist Protect officers and the CRC network, noting the importance of alignment with ministerial focus on public resilience. Officers advised that CRCs would shortly move fully under policing control, with significant work underway to transition from the current private-sector model.

A Member asked about fraud and Pursue activity and suggested that before-and-after examples be provided to demonstrate the impact of the FRACAS system. The Chair clarified that the focus was on ensuring that clear, measurable impact were captured on an ongoing basis to provide evidence for future investment.

A Member sought clarification on data availability during the transition between systems, noting concerns about a nine-month period without visibility. Officers confirmed two issues: low compliance and clarity across forces in recording items such as crypto seizures within JARD, and broader system difficulties. Officers advised that improvements were being explored, including using data from private-sector storage partnerships in the short term, but that consistency could not be fully achieved until the ARIT system was implemented.

The Chair noted the importance of asset recovery and requested a future deep dive to establish the baseline, new normal, and opportunities for improvement.

A Member asked about opportunities to further develop CRCs and their alignment with national responsibilities. Officers advised that a network of national ambassadors was already in place and that an update on the new CRC model and structure would be provided at a future meeting. Officers confirmed that engagement with IG and Mansion House colleagues was underway to widen ambassador outreach and noted recent references to CRCs in the Lord Mayor's speeches.

RESOLVED - That the report be noted.

5. **SUMMARY OF ACTION FRAUD PUBLIC COMPLAINTS DATA – Q2 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 2 2025/26 (1 July 2025 – 30 September 2025).

A Member noted that outcomes from previous complaints had been requested at the last meeting but were not included in the report. Officers confirmed that this information could be provided for the next meeting and noted that no appeals had been upheld in the current period. The Chair observed that the absence of upheld complaints could also be a matter of concern and requested that Officers review the presentation of complaint outcomes to ensure that Members received appropriately informative data.

A Member also noted an increase in complaints submitted by MPs and asked that all MPs raising concerns receive information about the Report Fraud system. Officers confirmed that MPs formed part of the target group for the forthcoming Report Fraud launch.

RESOLVED - That the report be noted.

6. **CYBER GRIFFIN UPDATE**

The Committee received a report of the Commissioner report of the Commissioner with an update on Q2 performance of Cyber Griffin. Members noted that it remains on track to have its highest performing year to date.

RESOLVED - That the report be noted.

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

There were no questions.

8. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
The Chair invited questions on the Action Tracker.

A Member observed that the Corporation's committee cycle did not always align with the Police timetable which on several occasions has led to deadlines for data analysis not being met. The Chair acknowledged the challenge but noted that discussions could be held with the Police Authority Team to see if a shift in timing was required. Officers were advised to raise any recurring difficulties with meeting scheduling as early as possible.

RESOLVED - That the action tracker be noted.

9. **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.

10. **NON-PUBLIC MINUTES**
RESOLVED - That the non-public minutes of the meeting held on 8 September 2025 were approved as an accurate record.

11. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**
The Committee received a joint report of the Town Clerk and the Commissioner on recent engagement to support promotion of the COLP's national roles and progress on developing the Salisbury Campus.

12. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE – REGULAR PROGRAMME PROGRESS REPORT**
The Committee received a report of the Commissioner on the soft launch of Report Fraud.

13. **DOMESTIC CORRUPTION UNIT QUARTERLY UPDATE**
The Committee received a report of the Deputy on the Domestic Corruption Unit (DCU).

14. **ECONOMIC AND CYBER CRIME ACADEMY RECOVERY PLAN**
The Committee received a report of the Deputy Commissioner concerning the Economic and Cyber Crime Academy Recovery Plan.

15. **ACTION TRACKER**
The Committee discussed this at Item 8.

16. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

17. **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 1.20 pm

Chairman

Contact Officer: Sorrel Cooper
Sorrel.cooper@cityoflondon.gov.uk

This page is intentionally left blank

Agenda Item 4

Reference	Meeting Date	Action	Exemption	Owner	Target Completion	Update	Status
ESCCC - 01	08/09/2025	Get the cadence of the packs better if possible – Q1 data being examined as early as possible in Q2. Use Red and Green to clearly indicate to all what is 'good' or 'not good'. Move towards One Performance Pack under ECCA relevant Policing Plan headings rather than Local /National / Policing plan separate packs.	Public	TG / MC / PA Team	16/02/2026	07/10/2025 - Packs are reported quarterly. This relates to the timeliness of committee meetings following the end of the quarter, Q1 is always challenging, and committee tends to be in September due to summer recess. Quarterly achieved status has been added to the pack for Q2.The move to one pack is being considered as a broader review of the performance frameworks aligned to National Lead Force, to ensure consistency and appropriateness in metrics with the ambition a revised pack will be for discussion later in 25/26.	In Progress

ESCCC - 02	08/09/2025	Move Complaints in Report Fraud to a % rather than a total number + clarity re 'complete population'	Public	MC / NC	16/02/2025	On-going	In Progress
ESCCC - 03	04/11/2025	**Action Fraud Complaints** - Include data on Action Fraud complaints being upheld or not	Public	TH	16/02/2026	25/11/2025 - Request sent across to P&T Team to consider 09/02/2026 - Paper is presented to the Committee	Completed
ESCCC - 06	04/11/2025	**Cyber Resilience Centre** - An update to be provided at the next meeting on the new model	Public	AG	16/02/2026	08/12/2025 - AG to lead on presentation / paper 09/02/2026 - Paper presented to committee	Completed
ESCCC - 07	04/11/2025	**Scheduling of meetings** - consider the scheduling of meetings for the next civc year to align with relevant quarterly reporting	Public	PA Team	16/02/2026	25/11/2025 - PA Team continue to work closely with CoLP to consider dates for next civic year 2026/27	In Progress

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee	**Dated:** **23 February 2026**
Subject: Deputy Commissioner's Update (National Leadership Functions)	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes**	People are safe and feel safe
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:	Deputy Commissioner Nik Adams
Report author:	DI Anna Martin

Summary

This report provides an update on National Leadership Functions from the Deputy Commissioner of the City of London Police.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. The following report outlines notable activity in the last quarter delivered by National Functions (City of London Police).

Current Position

2. As below

Options

3. None – for information only

Proposals

None – for information only

Key Data

The following the Deputy Commissioner's strategic update for this period;

Staffing

Commander Tor Garnett will be going on a period of leave prior to maternity leave from mid-February. T/Commander Oliver Shaw will be covering her role until her return.

Strategic Leadership and Engagement

Activity during the last quarter has focussed predominantly on the launch of Report Fraud which has now been successfully complete. As the project transitions into the next phase, I am sure you will join me in congratulating Chris Bell and his team on this momentous achievement. Further detail will provided in a separate agenda item.

In early December, Deputy Commissioner Adams attended the Global Anti Scams Alliance (GASA) conference in New York with senior CoLP, NECC and Home Office colleagues. The contingent also participated in a variety of bilateral meetings with US law enforcement and industry partners, gaining a broader understanding of their anti-scam centre approach.

Planning for the 1SS project continues in earnest and strategic engagement across various forums is ongoing. On 27th January Deputy Commissioner Adams spoke at a Parliamentary breakfast event which was well received. Further engagement events with organisations such as CIFAS, the Payments Association and TechUK are imminent.

February will be a busy month with the launch of the eagerly awaited new fraud strategy. Having undergone its public launch last month, the parliamentary launch of Report Fraud will also be taking place, most likely on the same day. CoLP are hopeful that much of the comprehensive feedback provided on the content of the Fraud Strategy will have been incorporated in the final version.

Members may have read Commissioner Pete O'Doherty's column article in the Times on 20th February where he extolled the benefits of the new Report Fraud service and advocated for further public-private collaboration in the fight against fraud and cyber crime moving forward.

The Commissioner, Deputy Commissioner and other senior CoLP staff will be attending the Global Fraud Summit in Vienna in March, hosted by Interpol and the United Nations Office on Drugs and Crime. This high-level event will bring together ministers and senior representatives from across governments, law enforcement, private sector, civil society organizations and international organizations.

In January Deputy Commissioner Adams, the PAB chair and CoLP colleagues welcomed Solicitor General The RH Ellie Reeves MP to GYE and had the opportunity to share with her the importance of CoLP's national leadership responsibilities.

At the end of January Dr Michelle Haslem, Director General Homeland Security Group, will also be visiting CoLP.

Operational Highlights

An insurance broker who abused his position of trust to divert payments totalling more than £133,000 into his own personal bank account has been sentenced to more than five years in prison, following an investigation led by the Insurance Fraud Enforcement Department (IFED). The offender used his role as an insurance broker to mislead customers, falsify documents, and misdirect payments intended for legitimate insurance policies. His actions left individuals and businesses without valid cover for homes, vehicles, and commercial property - placing them at serious risk. He was sentenced in November at Inner London Crown Court a total of five years and three months in prison.

Two PIPCU officers received an award from the United States Officer of the Inspector General from the Department of Motor Vehicles (US Government) in recognition of their successful investigation into the sale of counterfeit airbags, a significant public safety issue. The investigation, conducted in partnership with Homeland Security Investigations, saw 3 suspects arrested from two addresses in which hundreds of counterfeit airbags were recovered, as well as £210,000 in cash. Of the three suspects, two are awaiting trial in the UK and one has been sentenced to prison in the US.

Project Capstone continues to develop and achieve some significant operational success. This is the NPCC cybercrime portfolio's commercialised, collaborative approach with the private sector to analyse and develop augmented online data, in order to identify OSOC threats and cryptocurrency confiscation opportunities that would not otherwise be attainable to UK Policing. The project has so far achieved crypto asset seizure opportunities in excess of £50 million, the seizure of around £5 million of USDT, relating to a UK-based fraud, the identification of over 20 UK-based cybercriminals, over 40 viable cryptocurrency asset seizure opportunities relating to UK-linked frauds and the identification of 10 high-level Dark Web drug vendors operating in the UK

Operation Callback 2 took place in November and December 2025. This was a London based operation run by the Metropolitan Police and support by CoLP targeting courier fraudsters based in the capital. Proactive policing tactics were deployed against fraudsters contacting vulnerable victims nationally and persuading them to hand over money or valuables to couriers. This was accompanied by extensive protect activity and media campaigns. Analysis of courier fraud data show overall losses nationally have slowly decreased over the past two years, with significant dips in offending levels during and immediately following operations such as this.

Planning continues in earnest for Operation Henhouse 5 in February, the annual month-long fraud intensification funded by the NECC and coordinated by CoLP. Participation from all forces and ROCUs, along with some partner agencies, is anticipated.

Media Highlights

Various outlets reported on a recent PIPCU operation targeting illegal Sky streaming services. Headlines such as “Massive UK crackdown just blocked millions from streaming Sky TV for free” led articles describing a major police operation to shut down a illegal streaming platforms. The operation took place last week in Manchester with four people arrested and £750,000 worth of equipment seized. The investigation was launched after Sky reported suspicious activity connected to a large-scale illegal streaming operation. Investigators identified individuals suspected of running an unlawful IPTV service that supplied millions of users across the UK. One suspect is alleged to have earned more than £3 million from the operation. Sky confirmed that the illegal service experienced widespread disruption nationwide.

Temporary Detective Chief Superintendent Amanda Wolf participated in a Times interview entitled “How Britain tried (and failed) to stop a £10 billion crimewave”.
This article set out some ways in which the new Report Fraud system will enhance the response to fraud using improved technology and AI.

Corporate & Strategic Implications –

Strategic implications – None

Financial implications – None

Resource implications – None

Legal implications – None

Risk implications – None

Equalities implications – None

Climate implications – None

Security implications – None

Appendices

- None

Deputy Commissioner
Nik Adams

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee	**Dated:** 23rd February 2026
Subject: Policing Plan Performance Report – Q3 2025/26	**Public Report:** For Information
This proposal: • **Delivers Corporate Plan 2024-29 outcomes** • **Provides statutory duties**	• 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 Q3 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 – National Delivery Plan Performance Report Q3 – 2025/26
- Appendix 2 – National Lead Force, City of London Police Performance Report Q3
- Appendix 3 – City of London Policing Plan Performance Report Q3 – 2025/26

T/Ch Insp Megan Cardy, Head of Force Performance, Corporate Services.

This page is intentionally left blank

CITY OF LONDON POLICE

National Policing Lead For Fraud

National Lead Force
City of London Police Performance Report

FY 2025/26

Q3: October – December 2025

A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

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.

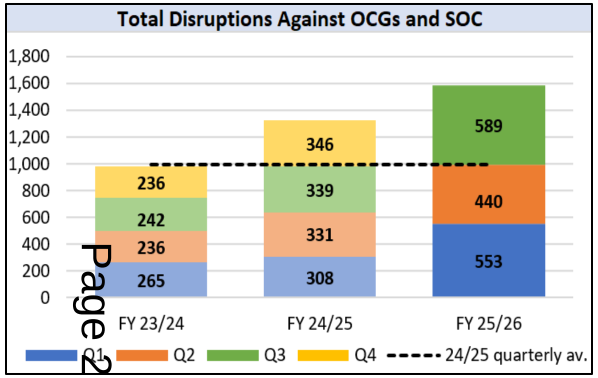
The NLF plan sets out **key cross cutting enabling commitments** that City of London Police is seeking to achieve:	FYTD Performance	Data Trend
We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS 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.	🟩	⇧

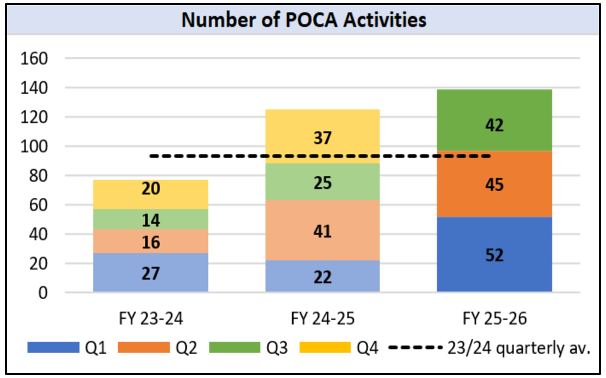
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

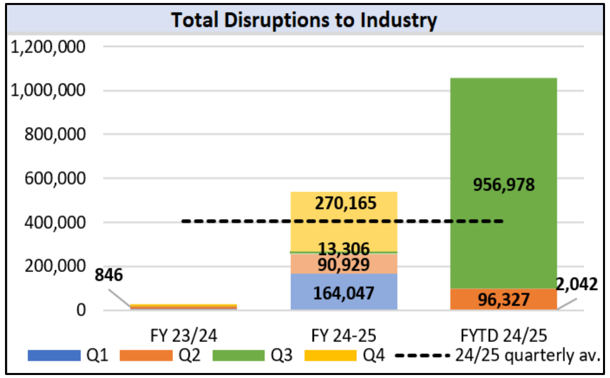
Proactively Pursue Offenders

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	🟩	⇧


Total Disruptions Against OCGs and SOC


Number of POCA Activities


Total Disruptions to Industry

OCG Disruptions

- Teams are investigating **79** OCGS (+11)
- In Q3 teams recorded against OCGs:
- **3 major** disruptions (-3 to 24/25 Q3)
- **28** moderate (+20 on 24/25 Q3)
- **66** minor disruptions (+54 on 24/25 Q3)
- **492** disruptions against other threats is a **57% (+179)** increase on Q3 24/25

Response **OCG Disruptions**

Fraud Ops led the increase in disruptions by adopting a 'proactivity in enforcement' mantra and an enhanced case adoption process. The FIT team also worked on developing knowledge and capability.

Financial Disruptions

- In Q3 25/26 Fraud Teams reported **42** POCA activities up **68% (+17)** from Q3 24/25 and 35% (+11) from the quarterly avg.
- These had a value of **£5,171,404** up **170% (+£3,257,903)** from Q3 24/25 and up 122% (+£2,837,965) from the quarterly avg.
- Activities included: **4** confiscations, **5** asset restraining orders, **18** cash detentions and **15** cash forfeitures

Industry Disruptions

In Q3 Fraud teams reported:

- **258** disruptions to websites
- **956,719** to cards and bank accounts
- **918** to social media and other
- **78% (+418,531)** increase on total disruptions in the whole of 24/25

Response **Industry Disruptions**

A **DCPCU** smishing fraud operation saw two suspects arrested. Their digital devices contained 942k sets of card/account details. The potential fraud saved was £195,610,767, an increase of 83% (+£89m) on the whole of 24/25 savings.

Response **OCG Disruptions**

Fraud Ops with support from CoLP Teams and the MPS disrupted a live courier fraud operation. This led to the execution of urgent warrants and the arrest, interview and bail of 4 suspects. The action disrupted the OCG's activities and prevented further individuals becoming victims. Two **PIPCU** DCs received an award from the US Office of Inspector General for their work into the international sale of counterfeit airbags, posing a risk to occupants in the event of a crash. Three suspects were arrested from two addresses where hundreds of counterfeit airbags were recovered, as well as £210,000 in cash.

Financial Disruptions

An **IFED** civil recovery case concluded with the forfeiture of £459,763. The funds were returned to the insurer, identified by the court as the principal victim of the fraud.

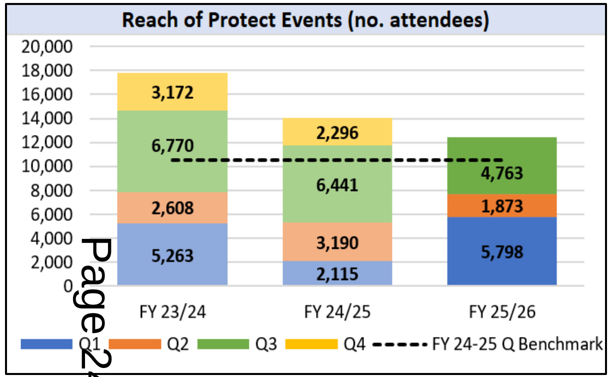
DCPCU investigated fraudulent orders though online auction houses. A suspect was arrested and devices seized, some containing crypto assets. Investigation identified accounts with significant funds that were frozen to prevent dissipation while the investigation progresses.

National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

Protect People and Businesses

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	🟥	⇩
C. Increase the number of Victim Care Unit contacts	🟩	⇧


Reach of Protect Events (no. attendees)

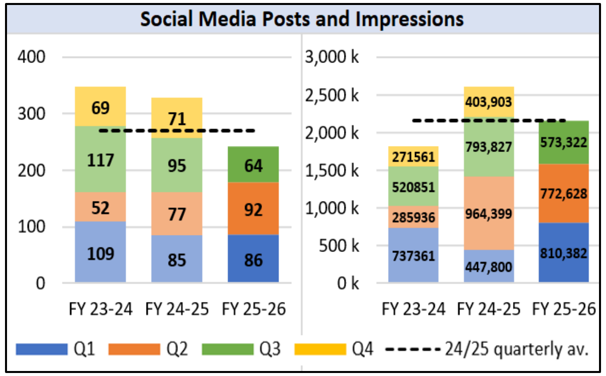
Protect Events

- Teams held **77** events in Q3 in line with Q3 24/25 **(+3)**
- **4,763** people attended these events down **26% (-1,678)** from Q3 24/25
- Activity peaked in November with **38** events & **1,511** attendees

Response **Protect Events**

DCPCU hosted a Virtual Industry Visit where members learned about the Unit.

IFED hosted their SPOC engagement day which brought together specialist teams from across policing and expert voices from the industry.


Social Media Posts and Impressions

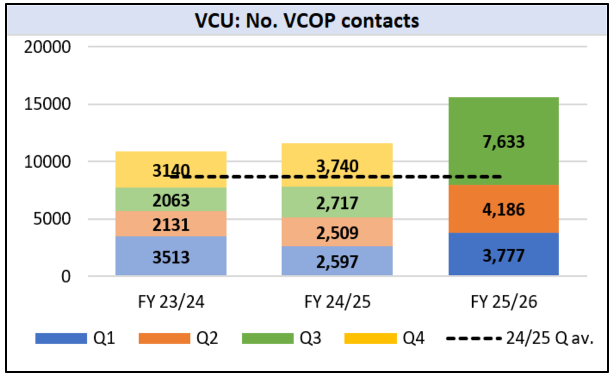
Social Media

- Teams posted **64** messages on social media, down **33% (-31)** on Q3 24/25
- The related impressions fell to **573,322**, down **27% (-220,505)** on Q3 24/25
- However, impressions are in line with the 24/25 benchmark over the year

Response **Social Media**

Posts have fallen in Q3 as the team focused on preparation for launching the Report Fraud Service.

Upcoming in Q4: All channels will be amplifying the launch of Report Fraud. It is hoped posts will return to normal levels.


VCU: No. VCOP contacts

Victim Care Unit

- VCU was responsible for **5,773** victims in Q3 up **22% (+1,043**) victims since Q3 24/25 relating to **28** (+2) investigations
- A total of **7,633** VCOP updates were issued, up **181% (+4,916)** from 24/25
- **2,206** 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 November, VCU participated in a Protect campaign.

Response

Social Media

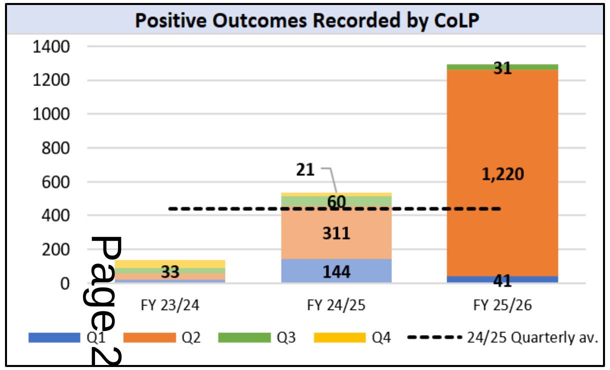
- **PIPCU** issued posts relating to confiscation orders granted against brothers who were sentenced for selling counterfeit items and following seizure of counterfeit car parts.
- **IFED** activity peaked in Nov with an intensification linked to Black Friday; focused on fraudsters who claimed their electronic devices had been damaged to secure payouts and fund newer models. Social media posts received paid spend on YouTube and Meta platforms.
- **NLF** urged the public to remain vigilant following a rise in payment diversion fraud, commonly known as conveyancing fraud and posted about Op Tonic, a romance fraud intensification.
- **DCPCU** gained high views for updates on significant sentencings such as a former bank employee sentenced to 12 months imprisonment for over £16,000 worth of fraud by abuse of position. After tricking elderly victims DCPCU were able to return the money which he had stolen.

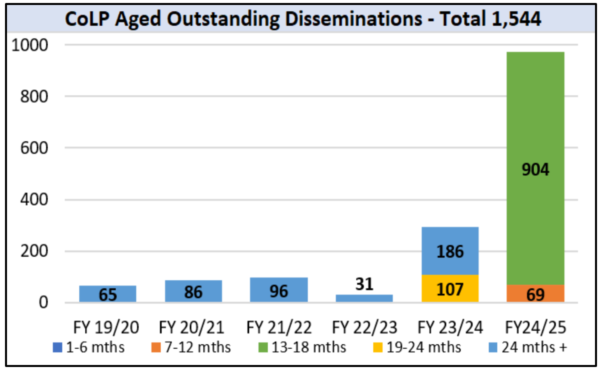
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

Improve Outcomes for Victims

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	🟩	⇧
B. Decrease CoLP aged outstanding disseminations	🟩	⇩
C. Support CoLP teams to engage in intensification efforts	🟩	⇧





Positive Outcomes

- In Q3 CoLP teams recorded **31** positive outcomes
- Down **50% (-29)** from Q3 24/25, and down **23% (-9)** from the 24/25 benchmark
- **63** 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 **33%** for Q3, an increase of **12%** from Q3 24/25

Outstanding Disseminations

- At the end of Q3 **1,544** disseminations from 19/20 to 24/25 were with CoLP teams awaiting outcomes
- This is down **27% (-558)** from the end of Q1 showing ongoing improvement and the impact of closing one large investment fraud case in Q2

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.

Intensifications

Operation Willrow was an intensification targeting false claims on insurance policies. The operation, in the lead up to Black Friday, focused on fraudsters claiming their electronic devices are damaged to secure payouts and fund newer models.
During the week, IFED officers issued 19 cease & desist notices. Officers also executed a warrant where approx. £15,000 in cash was seized. A paid advertising initiative was run on Meta and Google platforms and reached 200,000 people, with high engagement rates.

Op Callback was an 8-week intensification focusing on Courier Fraud. It ran for 8 weeks in Oct and Nov. CoLP provided coordination, backup resources, and Intel support.

Response **Intensifications**

HENHOUSE 5, will be a fraud intensification coordinated by the NECC and CoLP, with intensified and coordinated PURSUE operational activity taking place throughout February 2026.

Response

Positive Outcomes

Total CoLP positive outcomes across all units remain flat with circa 11 returns a month on average, excluding large one-off operations. However, the pipeline remains strong.

Q3 for CoLP reflected a return to BAU volumes of positive outcomes in line with Q1. In Q2, NLF CoLP recorded an Investment Fraud which yielded 1,199 positive outcomes. There are a number of ongoing investigations of Investment Frauds within CoLP, which are young and at a pre-charge stage, with a combined total of at least 1,200 victims. These are expected to come to a conclusion in 1-2 years.

Positive Outcomes have been calculated using the legacy systems rather than the new National Crime Analysis System (NCAS) this quarter. Analysts are working on the reporting of outcomes recorded in NCAS and these will be added to legacy outcomes from Q4 which may increase Q3 totals. Additional information is provided on Slide 7.

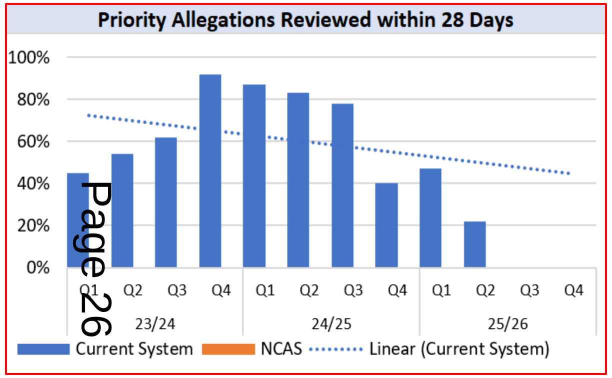
National Reporting Service: Includes Report Fraud Reporting Service, Analysis Service and Victim Services

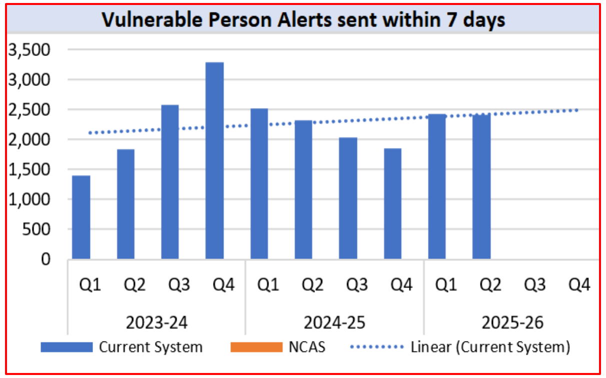
Proactively Pursue Offenders

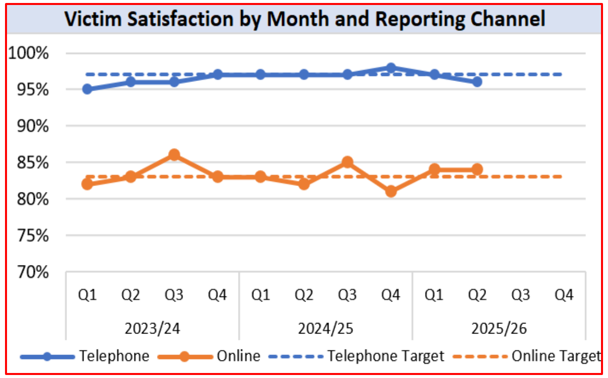
We will deliver the Fraud and Cyber Reporting and Analysis Service (FCCRAS) - including the ability to feedback intelligence into the system for further development and inclusion in intelligence packages. We will ensure intelligence is appropriately recorded and disseminated to assist with all 4P outcomes

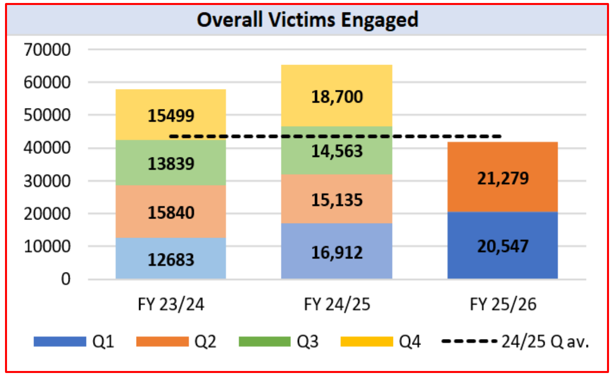
Success Measures:

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. Maintain the percentage of survey respondents who are satisfied with the Action Fraud reporting service
D. Increase number of fraud victims who receive protect advice (NECVCU engagement)









Report Fraud - Reporting, Analysis and Victim Services

The delivery of Report Fraud Reporting Analysis and Victim Services went live on 4th December 2025 with a public launch on 19th January 2026. The data platforms and reporting processes are still being refined and it has not been possible to provide like for like information to be reported on for this performance product.

Victim Satisfaction

However early indications between Go Live and 31st December 2026 are that 82% of people completing the survey after reporting online agree that they “would feel confident using the Report Fraud service if they needed to again”. However this does reduce to 31% of people completing the survey after receiving an outcome of their report. It is believed this is linked to non-disseminated reports however this is being investigated further.

Please note no Q3 data is included in the above graphs and therefore success measure status has not been included.

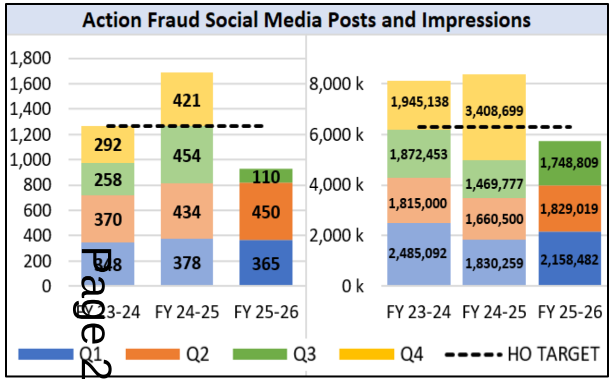
National Reporting Service: Includes Report Fraud Reporting Service, Analysis Service and Victim Services

Improve Outcomes for Victims

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:

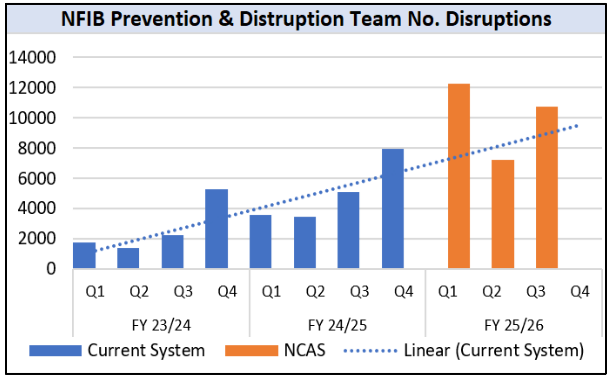
A.	Increase the number of Action Fraud social media posts and impressions	🟨	⇨
B.	Increase the number of NFIB P&D disruptions	🟩	⇧



Action Fraud Social Media

- AF made **110** posts in Q3, down **76% (-344)** from Q3 24/25
- The related impressions for these posts totalled **1,748,809** an increase of **19% (+279,032)** from the previous year
- The focus on fewer campaigns meant less posts, but the paid activity increased impressions and engagement

<u>Response</u> **Action Fraud Social Media**
Activity in Q4 will focus on the launch of Report Fraud from mid-January.



Preventions and Disruptions

- In Q3 the NFIB P&D team carried out **10,767** disruptions, double that of Q3 24/25 **112% (+5,700)**.
- Disruptions included:
- **563** website disruptions
- **768** email account suspensions
- **105** telephone deactivations
- **9,287** proactive domain suspensions
- **44** social media account suspensions
- Growth is particularly evident with proactive domain suspensions since the team started to use the National Crime Analysis System (NCAS).

<u>Response</u>

Action Fraud Social Media

Social media activity focused on two campaigns this quarter:

National Cyber Security Month – October
During the month, Protect advice was shared and promoted e.g. protecting online accounts by enabling 2-Step Verification and creating strong passwords. The campaign used a video reel in partnership with Meta who funded the paid social media activity. The link signposted was clicked 7,312 times which is 100% higher than an organic post. The posts were used over 185 time on X by partners and police forces.

Black Friday/Cyber Monday – 24th November
This campaign was done in partnership with the National Cyber Security Centre and Stop Think Fraud to help the public to shop safely online. The Campaign reached over 1.8 million people across the UK with 2.8 million impressions. The social media assets were used 114 times by partners and polices forces.

<u>Response</u>

Prevention & Disruption

Increased performance by the Prevention and Disruptions team in Q3, particularly in Proactive Domain suspensions (Horizon Scanning / Nominet Alerts) is a result of

- a proactive lens,
- forward thinking,
- being alert to the increase in fraudulent fake shop websites and other fraudulent websites in the lead up to Christmas, and
- proactively targeting newly registered domains likely acting maliciously in this space.

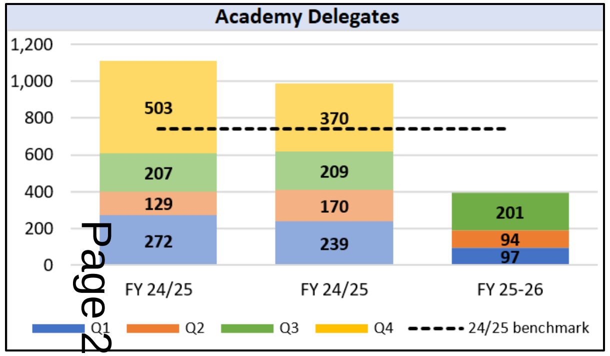
In relation to reactive disruptions, the 'high harm enabler list' on NCAS prioritises crime types likely to cause the highest harm . By focusing on these crime types, the Team are able to minimise the harm caused to victims, disrupt offenders and protect future victims.

Economic Crime Police Headquarters: Includes Workforce Strategy, Economic Crime and Cyber Academy and Protect.

Protect People and Businesses

We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber c rime. 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).	🟥	⇨
B.	Deliver objectives against National Workforce Strategy.	🟩	⇧
C.	Provide forces who are due to be inspected with specific pre-inspection support for delivering against the Fraud pillar within the PEEL framework	🟩	⇧



Academy

- In Q3 the ECCA held **16** courses, down **11% (-2)** from Q3 24/25
- At **201** delegate numbers were down **4% (-8)** from Q3 24/25
- **90%** satisfaction was equal to Q3 24/25 and the benchmark

Response Academy

In Q3 the 1st AMLAR-funded Money Laundering course was delivered, with 8 scheduled for delivery in 2026. The ECCA has a comprehensive schedule of courses planned through to the end of the financial year.

Reasons Academy

Numbers of both courses and delegates rose month on month throughout the quarter to be in line with the previous year, with delegate numbers doubling from the first half of the year. These sessions engaged participants from 13 different UK police forces, reflecting continued national reach; and saw an increase in public sector participation, primarily driven by requests for closed courses. The satisfaction rate experienced fluctuations during the period, with declines attributable to venue-related issues, which were quickly resolved. Importantly, the feedback did not reflect any concerns regarding course content or instructional quality.

Workforce Strategy

Highlights from prioritised workstreams under the National Policing People Strategy for Fraud, Economic and Cyber:

1. **Direct Entry Detectives** – good progress on new pathway to recruit detectives who will focus on economic or cyber crime in partnership with Police Now.
Cohort 1 - 12 CoLP officers started March 2025
Cohort 2 - 8 CoLP officers to start in March 2026.
Cohort 3 - Planning underway with CoLP and partner forces (exact number TBC) to expand programme outside CoLP.

2. **FIO Student Placements** – Planning for expansion of scheme to further ROCUs and forces for *Cohort 3* starting in Sept 2026.
Cohort 1 – 2 Students within CoLP in their part time year.
Cohort 2 - 12 students on their placement years are now embedded within 4 ROCUs, MPS, and CoLP.

3. **Volunteers** – Funding agreed through the Cyber portfolio for two secondments (Chief Inspector and Police Staff Deputy) to lead the national programme. Candidates in vetting/ onboarding. A T/Inspector joined the team to lead on volunteers within CoLP & support the national project.

Complete workstreams include Career Pathways video for CoLP detailing key roles within Economic Crime, a Pay Parity Report, the inaugural Challenge Panel for practitioners on the Fraud Investigation Model, and the launch of the Living Library.

NCO - PEEL Support

Force visits are predicated on direct requests for support in anticipation of upcoming HMICFRS visits. The NCO are not seeking to coach or mentor forces through those inspections but are providing forces with advice and guidance as to what good practice is when formulating a response to fraud.

On 14th October 2025 a Fraud Lunch and Learn Session was hosted by Commander Garnett. All Chief Officer Teams from across the country were invited to the virtual event which was well received. The content of the event was matched closely to the key elements of advice being shared with forces through NCO engagement.

15 force engagements were held in Q3 up **150% (+9)** from the 6 held in Q2. 3 further engagements have been planned for January 2026.

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Lead Force
National Delivery Plan Performance Report

FY 2025/26

Q3: October – December 2025

A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

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

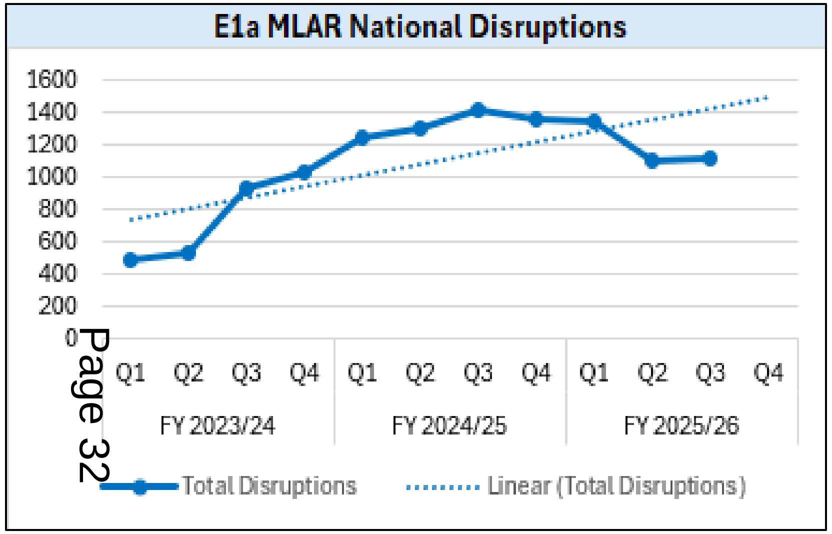
		FYTD Performance	Data Trend
Cyber 1	We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB 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.	🟥	⇩

Money Laundering and Asset Recovery

Improve Outcomes for Victims

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

Success Measures:	FYTD Performance	Data Trend
E1a Increase the number of recorded disruptions linked to money laundering and or illicit finance – **Home Office Measure**	🟩	⇧


E1a MLAR National Disruptions

Op Machinize 2

Operation Machinize 2, led by the National Crime Agency (NCA) ran throughout October and targeted economic crime on the high street with businesses being used as a cover for a wide range of criminality with a real focus on the laundering of funds from that criminality.

This operation involved 2,734 premises visited, 923 arrests and £538k of cash seizures. So far nationally there have been 226 disruptions under the name Op Machinize for Q3.

Analysis

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

In Q3 (October – December), there were a total of 1,117 disruptions.

- 71 major disruptions - 15% increase (+9) in comparison to Q2 25/26
- 170 moderate disruptions - 4% decrease (-7) in comparison to Q2 25/26
- 876 minor disruptions - 1% increase (+9) in comparison to Q2 25/26.

The top 3 disruption types are asset denial & ancillary orders at 51% (690), seizures at 20% (273) and investigative suspect disruptions at 13% (171).

In comparison to the previous quarter (Q2), MLAR disruptions are reporting a 1% increase (+11). In comparison to the same quarter for the previous year (Q3 24/25), there has been a 21% decrease (-294) in MLAR disruptions.
The benchmark from 24/25 is 5,323, which translates to 1,331 disruptions per quarter. For Q3, disruptions are 10% (-418) below the benchmark target, however, disruptions have increased compared to the previous quarter.

Response

In Q3, operational activity contributed to a rise in disruptions, in particular Op Machinize 2. This was the largest operation of its kind focused on rooting out the economic crime and grey economy that makes our high streets less safe and prosperous.

Issues with properly recording disruptions is still on-going, attributing disruptions to the correct operations and ensuring operation names are added upon entry. This can give better insight into the outcomes of intensifications and operations to allow for best practices to be identified. The work to continue this continues to be a key focus of the NPCC Serious and Organised Crime portfolio and COLP is working with the NCA to support this across policing colleagues where possible.

This is a continuing recording issue and not a direct performance issue relating to MLAR disruptions.

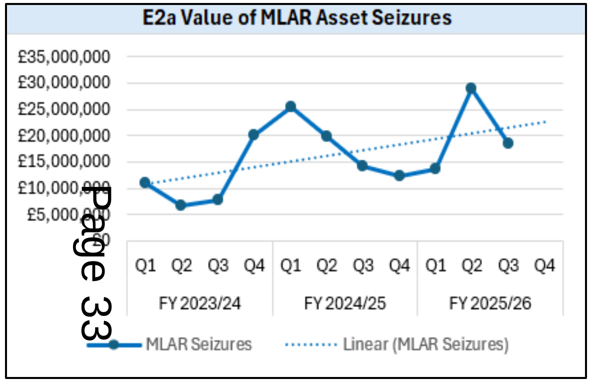
We are expecting to see a rise in disruption activity continue Q4 as planned operations take place and as disruptions are recorded against Op Machinize 2 as investigations progress.

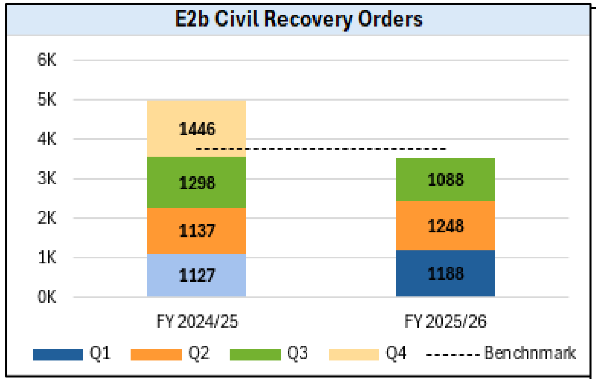
Money Laundering and Asset Recovery

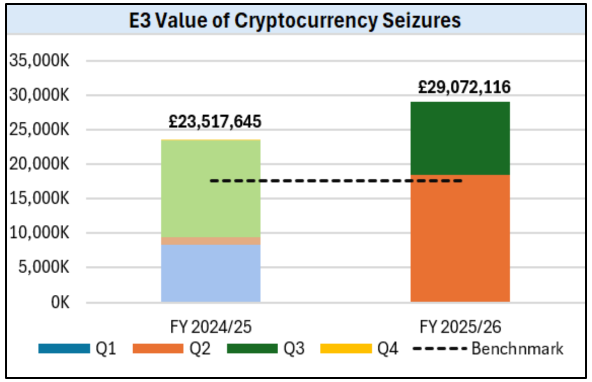
Proactively Pursue Offenders

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 Q3 (October – December), a value of £18,615,212 asset seizures was recorded for money laundering and asset recovery. In comparison to the previous quarter, this is a 36% decrease (-£10,386,302), however Q2 was a highest reporting quarter in the previous three years. In comparison to the same quarter for the previous year (Q3 24/25), this is an 30% increase (+£4,301,737). For 24/25, asset seizures were reporting a downward trend, 25/26 has shown improvement and is 13% above the Q3 benchmark for 24/25 (+£7,177,156). Asset seizures are opportunity-driven, intelligence led and legally constrained which can cause sporadic data trends. Op Machinize 2 reported £2,789,515 in estimated seizure value for Q3, this accounts for 15% of seizures for Q3.

E2b Civil recovery figures in Q3 are reporting a 13% decrease (-160) in comparison to the previous quarter (Q2) and a 16% decrease (-210) in comparison to same period in 24/25 (Q3). Q3 is reporting 6% below the quarterly benchmark for 24/25, although Q3 was a low month, we are maintaining consistent levels of civil recovery orders.

E3 For Q3, there has been £10,611,753 in cryptocurrency seizures, overall, the Q3 benchmark is £17,638,234, Q3 is reporting 65% above the target (+£11,433,882). Although Q3 is reporting a 42% decrease in comparison to Q2, Q2 was a very high month for cryptocurrency seizures and overall, 25/26 is reporting a large increase, surpassing the benchmark for 24/25.

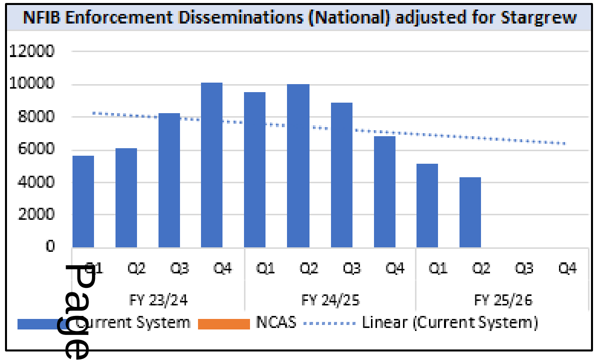
Cryptocurrency seizure figures are currently reported here in the same way as disruption activity via the APMIS tool hosted by the NCA. This is not the ideal reporting method and this causes limitations in what can be reported as well as concerns over accuracy of data reporting. More work is on-going to obtain data from Komainu the national crypto currency vault and the introduction of a new Asset Recovery reporting tool (ARIT) later in 2026 will improve reporting capabilities and performance understanding significantly.

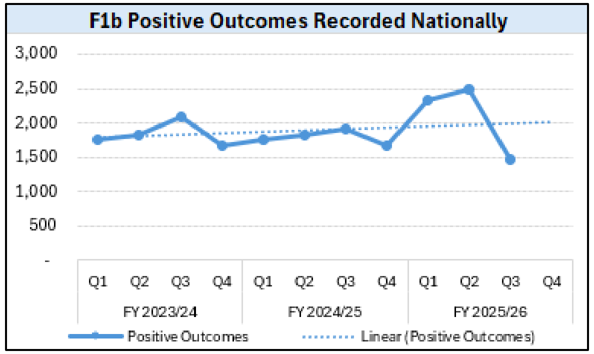
Fraud

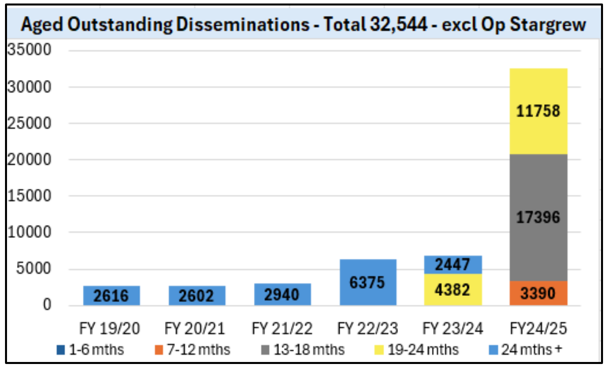
Improve Outcomes for Victims

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		
F1b Improve the positive outcome rate		
F1c Reduce the percentage of crime disseminations not yet assigned an outcome	🟩	⇧


NFIB Enforcement Disseminations (National) adjusted for Stargrew


F1b Positive Outcomes Recorded Nationally


Aged Outstanding Disseminations - Total 32,544 - excl Op Stargrew

Please note no Q3 data is included in F1a and F1b graphs have been calculated using the legacy systems rather than the new National Crime Analysis System (NCAS) this quarter and will only represent partial outcome volumes, therefore success measure status has not been included. The delivery of Report Fraud Reporting Analysis and Victim Services went live on 4th December 2025 with a public launch on 19th January 2026. The data platforms and reporting processes are still being refined and it has not been possible to provide like for like information to be reported on for this performance product. However some initial data Total number of Pursue Packages Disseminated between Go live on the 31st December 2025 1120 with 1963 crime reports within them. 371 of these were automated Call for service disseminations which previously would have required a manual review and input from the service.

F1b Nationally, there have been 1,478 positive outcomes during this period and 9,177 no further action outcomes. Overall, there is a 13% positive outcome rate. This is a 7% decrease on Q2 24/25, with a positive outcome rate of 20% and a 5% decrease in positive outcomes in comparison to the same period for the previous year (Q3 24/25). The quarterly target of 3,571 has not been met and positive outcomes are reporting 36% below the benchmark for Q3 (-1,270).

F1c In Q3, **32,544** NFIB disseminations from 19/20 to 24/25 had not been matched to an outcome. This is a decrease (which is positive) of 3% (-1,105) from the previous quarter and an increase of 8% (-2,523) from Q3 24/25. 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.

Outcomes

Against the comparative period last year positive outcomes in the legacy system for Q3 were down by 38%, (-889).

This is due to Q3 25/26 not containing any large one-off cases from forces, thus averaging circa 500 per month (i.e. a run rate of circa 6,000 per annum).

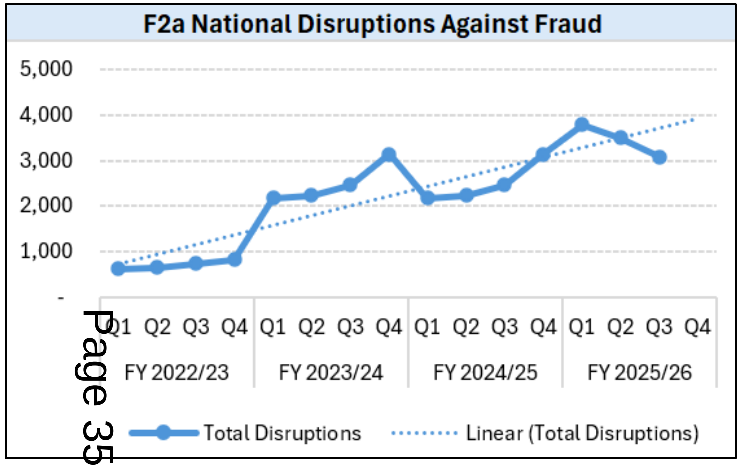
For the year to date 9 months to 31st December 2025, total positive outcomes were **6,340**, up **122 (+2%)** on the prior year
Key drivers across the first 9-month period include an Investment Fraud operation from NLF CoLP yielding 1,199 outcomes in September.

Fraud

Proactively Pursue Offenders

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	🟩	⇧



Op Callback 2
Op Callback was an 8-week intensification focusing on Courier Fraud, this operation resulted in 37 disruptions for Q3. (More details on Op Callback 2 in slide 9)

OP ROME - NEROCU
Op Rome involved raising awareness of financial crime amongst business and communities. Messaging was provided direct to employees promoting vigilance around the human element of fraud and common economic attacks. Officers encouraged tactics, behavioural change and understanding of risks. This operation resulted in 119 minor disruptions for Q3, the largest reported disruption recording for this quarter.

F2a Nationally, there were 3,074 disruptions recorded for Q3 (October-December). Q3 was a low reporting month with a 12% (-421) decrease compared to the previous quarter. Q3 is reporting a 25% increase (+607) in comparison to the same period for the previous year and is 38% (+2,846) above the quarterly target, therefore, overall disruption performance is good.

For fraud related disruptions there were:

- 16 major disruptions - 41% decrease (-11) in comparison to Q2 24/25.
- 161 moderate disruptions - 13% increase (+19) in comparison to Q2 24/25.
- 2,897 minor disruptions - 13% decrease (-429) in comparison to Q2 24/25.

Overall, adult safeguarding is the highest disruption type at 36%, followed by specialist advice at 24%. Investigative suspect disruptions also reported high level disruptions at 11%.

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.

Response
Disruption performance has decreased, however overall, is reporting above the benchmark. This decrease was expected as outlined in the Q2 pack as the NPCC Serious and Organised Crime portfolio and national leads reset expectations around reporting across all of the Serious and Organised Crime landscape to ensure consistency in recording nationally which previously had been unreliable.

This decrease may continue in to Q4 as new normals are established aligned to the reporting change however operational activity is still on-going with Op Callback 2 data still being analysed, this will lead to an increase in disruptions being reported in Q4 aligned to this specific operation alongside Op Henhouse which is due to take place in February and has previously resulted in significant volumes of disruptions.

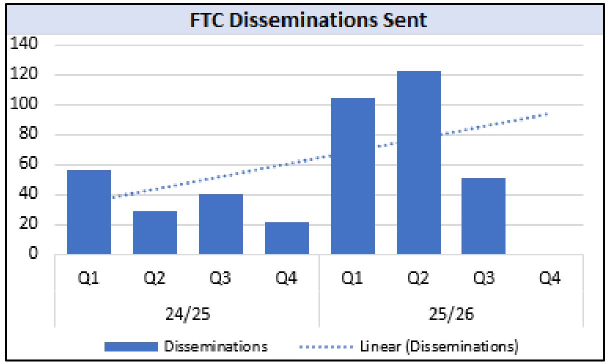
Fraud

Proactively Pursue Offenders

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	🟩	⇧
F4 Increase the number of Fraud Targeting Cell (FTC) packages allocated, adopted, and investigated	🟥	⇩

F3 In Q3, **Op Callback 2** took place, this was an 8-week intensification focusing on 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 was a joint operation working alongside the Metropolitan Police. Currently data is being analysed but the Metropolitan Police have reported 33 arrests, 9 subjects charged, 61 serious and organised crime disruptions and £55,000 in cash seized. This intensification also provided links to two other on-going operations involved in courier fraud, identifying two distinct modus operandi involving courier fraud.
Op Tonic took place from 29th September – 5th October. This was a one-week Romance Fraud intensification initiative, for "World Romance Fraud Scam Prevention Day" on the 3rd October 2025. The primary aim was to raise awareness, deliver protect advice and encourage reporting of romance fraud. This also involved collaboration and joint working with Barclays fraud and scam vans in engagement days. This intensification reported 2,299 posters distributed nationally, 12 engagement days, 61,142 impressions recorded on Facebook by Report Fraud and 405,516 social media impressions reported from forces. Overall, given the short timescale and limited resources, the fraud network pulled together collaboratively to promote romance fraud awareness on a national level. They delivered some great events and engaged with the public successfully.



F4 In Q3 a total of 51 disseminations were sent by the Fraud Targeting Cell (FTC). This is a 58% decrease (-71) compared to Q2 of 24/25, and a 28% increase (+11) compared to the same period for the previous year. The main driver for this due to the significantly higher number of disseminations that were sent out as part of Operation Barton in the previous quarter.
There have been several great outcomes for FTC for this quarter such as Op Barton which resulted in 2 moderate disruptions and 31 criminal investigations. In September, Op Lily produced 9 additional subject profiles and following these disseminations, 6 subjects have been interviewed with visits upcoming for the following 3 subjects.

Response

Intensifications

In Q3, Op Henhouse 5 is set to take place in February. This will see coordinated pursue and protect activity across all 43 police force PSNI, Police Scotland, every regional organised crime unit, Trading Standards, FCA and NCA, SFO and Insolvency Service.

This year we have £880K committed for operations across all 43 forces, PSNI, Police Scotland, every region and across Trading Standards, FCA and NCA, SFO and Insolvency Service. CoLP are also leading on an intelligence lead operation with FTC and private industry threat intelligence taking action against 10 UK centric fraud enabling telegram channels. These groups have circa 30,000 members sharing compromised data, tools and tradecraft, benefiting from the anonymity such platforms provide to enable hundreds and thousands of frauds against UK victims.

FTC

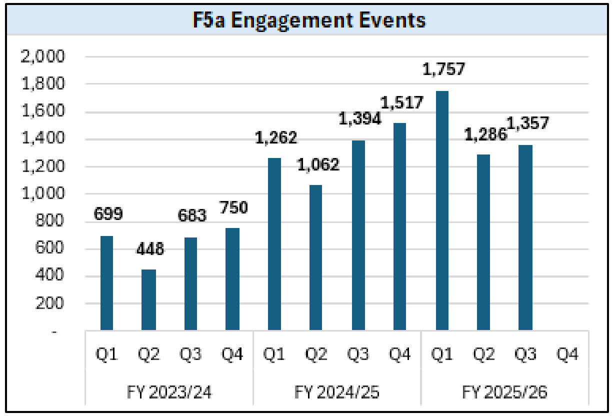
Progress on Op seraphim has been made with intelligence products relating to cybercriminals advertising fraud enabling products on Telegram channels. Currently work is on-going with Nigerian law enforcement and the Proactive Economic Crime Team (PECT) network. Close work is also on-going with the Cyber Defence Alliance to identify and attribute the cybercriminals.
FTC alongside Rick Nolan and the PECT Coordinator, have been having discussions with Flashpoint, a Cyber Threat intelligence company, around assisting in the attribution of the entities to cybercriminals.

Fraud

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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	🟩	⇧
F5b Percentage of protect engagement event attendees satisfied with the engagement they attended	🟩	⇧
F5c Percentage of protect engagement event attendees likely to change their behaviours as a result of engagement	🟩	⇧



F5a For Q3, **1,357 engagements** were held across the network, with **245,507 attendees**. Q3 is reporting a 6% (+71) increase in comparison to the previous quarter and a 3% (-37) decrease on Q3 24/25.

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 FQ3, **96%** were very satisfied and satisfied with the event/engagement (2% decrease from Q2)
97% were likely to change their behaviour or already undertake that behaviour (2% decrease from Q2).

In Response
The network continue to utilise the fraud protect surveys during their presentations, events and interactions with citizens and businesses across the country to understand engagement impact. The National Lead for Protect and the Home Office have emphasised to the Regional Coordinators how important they are. Staff consistently receive high praise from attendees for the quality of information shared, and their delivery.

In Q3, as part of **Op Tonic**, Report Fraud Protect Services coordinated a partnership with Barclays who have a fleet of vans that go to various locations to provide banking services to the community, these also offer mobile fraud awareness sessions. During the romance fraud intensification week, several protect officers from various regions joined the Barclays staff in the vans to promote romance fraud awareness (as well as general fraud awareness).

In October, for **Cyber Security Awareness month**, the Protect team focused on promotion of a promotional video in partnership with Meta on 2 Step Verification. The social media campaign reached over 300,000 people with 637,904 impressions.

The **Online Shopping Campaign** launch on the 24th November to help the public to shop safely online. This campaign was done in partnership with the National Cyber Security Centre and Stop Think Fraud aligned to the black Friday shopping events and the online shopping increase during the festive period.
The Online Shopping Campaign reached over 1.7 million people across the UK with 2.8 million impressions. The social media assets were used 114 times by partners and polices forces.
The Action Fraud Parr of the Online Shopping Campaign had over 300,000 impressions and 2,000 reactions across Instagram, Facebook and X.

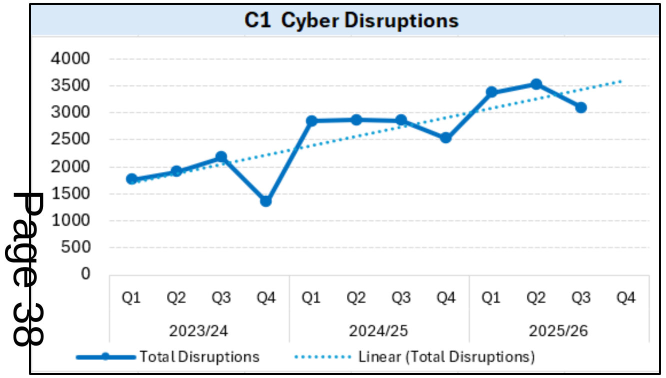
For Q4, the Protect team will be collaborating with SWROCU on proactive romance fraud and victim protect notifications.

Cyber

Improve Outcomes for Victims

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)	🟥	⇩



C2. For Q3, there have been no 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.

C1. In Q3, there were a total of 3,089 disruptions.

- 7 major disruptions - 600% increase (+7) in comparison to Q2 25/26
- 75 moderate disruptions - 17% increase (+11) in comparison to Q2 25/26
- 3007 minor disruptions - 13% decrease (-459) in comparison to Q2 25/26.

In comparison to the previous quarter (Q2), Cyber disruptions are reporting a 13% decrease (-442). In comparison to the same quarter for the previous year (Q2 24/25), there has been an 8% increase (+231).
For the Q3, disruptions are reporting 20% (+1,680) above the benchmark, although Q3 reported a reduction is disruptions, overall disruptions have been increasing year on year and are on an upward trend.

The top 2 disruption types are specialist advice at 66% and safeguarding at 16%. 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.

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. Q3 25-26 has seen 20 additional intelligence packages disseminated to the ROCU & Proactive Economic Crime Teams (PECT) network. All packages have been accepted by the network and are currently under development. A formal tasking and feedback process continues to be formalised with ROCU leads. Q3 reported seizures more than £1 million of various cryptocurrencies from across the ROCU networks.
During Q3, Project Capstone shared its methodology with Report Fraud and worked collaboratively to identify viable suspects and investigative leads at scale for forces and regions.

Response

Overall, the number of major and moderate disruptions has reduced in 25/26 compared to the same period 24/25. The only strand to see a national increase is Prepare. Individually and reversing this trend is the Northeast ROCU who've seen a significant increase in Protect disruptions during 25/26.

This rise stems from OP ANZAC, a regional project that proactively uses Police Cyber Alarm to identify cyber threats actively posing a risk to businesses. These police interventions prevent potential network intrusions, data exfiltration, and system compromise.

The NPCC Serious and Organised Crime portfolio continues its review of APMIS consistency across all SOC (including fraud and cyber) recorded disruptions which is impacting disruptions recorded as has been highlighted in other pages.

The restructure of the Network, to consolidate the CRC and bring under the direct leadership of the NPCC National Cybercrime Team has been a focus this quarter an d has impacted referral mechanisms and subsequently operations page 12 covers this in greater detail.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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.

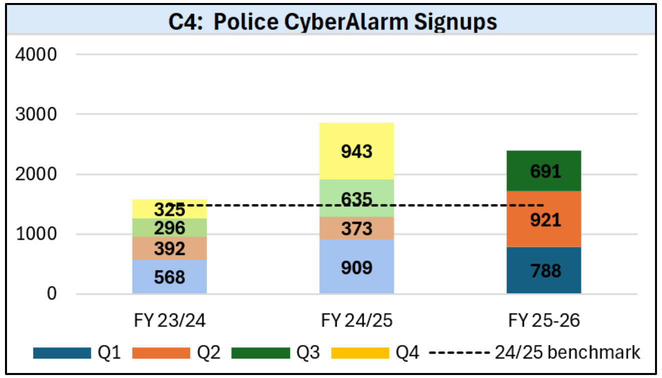
Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police Cyber Alarm to help support member organisations when issues are i dentified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police Cyber Alarm to all SME organisations 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 Q3, the network reports 105 disseminations, of which 103 (98%) were completed within the quarter. Of the Q1-Q2 25/26 disseminations, 49% related to ransomware and 27% a data breach; the main industries tasked out to were Retail/Trade, Manufacturing, Information and Communication, and Financial and Insurance.

Protect Notification outcomes are captured, helping to improve the recording of cybercrime in the UK and quantify the impact of the Protect network; 37% of the Q1-Q2 25/26 taskings have confirmed incidents and crime reports raised.



C4 In Q3 25/26, 691 Small to Medium-sized enterprises (SMEs) signed up to Police CyberAlarm. This is a 25% decrease (-230) in comparison to Q2 and 9% increase (+56) in comparison to the same period for the previous year (Q3 24/25). Overall, performance is reporting 12% above the 24/25 benchmark (+255).

Response

Police CyberAlarm (PCA) is undertaking a change of vendor to Waterstones Ltd. 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. As a result of this change, several functionalities within the system have been disabled within the current system a transition is planned from the old system to the new system.

As a result of this change, several functionalities within the system have been disabled within the current system a transition is planned from the old system to the new system.

Waterstons Ltd are developing a brand-new, custom-built system for Police CyberAlarm which will deliver improved and increased functionality. The new system is expected to be launched in Q1 of 2026-2027. However, until this available, one of the functionalities that has been disabled are Notification Packages for law enforcement. Member organisations are still able to register, download, install and configure the current system which enables them to receive their monthly threat and vulnerability reports.

Active promotion of the current version of Police CyberAlarm has ceased until we move closer the launch of the new system, alongside the new system will be a new public facing promotional website and Customer Relationship Management (CRM) solution.

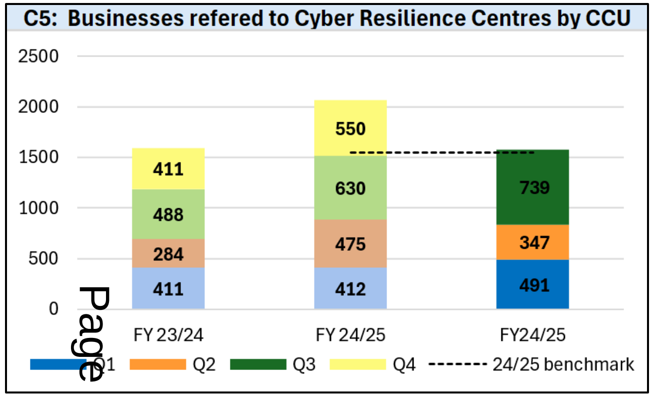
Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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: Businesses refered to Cyber Resilience Centres by CCU



C5

In Q3, the number of Cyber Resilience Centre (CRC) referrals increased by 113% (+392) in comparison to the previous quarter.

Referrals have also increased by 17% (+109), in comparison to the same quarter for the previous year (Q3 Q4/25). Overall, figures are reporting 2% (-26), under the benchmark for this quarter, however Q3 is the highest quarterly reporting month to date.

Response

The restructure of the network, to consolidate the limited companies and bring under the direct leadership of the NPCC National Cybercrime Team was delayed, but is now nearly complete, with the final two regional CRCs expected to close and transfer assets in January 2026. The new operating model, strategy and national delivery plans have been implemented, with regional CRCs creating a regional plan to deliver on the strategic objectives, alongside local priorities. The new KPIs for the network are under consultation with key partners, but are likely to be:

1. Membership growth (particularly in priority sectors)
2. Number of 30 minute 'cyber health checks' completed
3. Number of referrals to, and engagement with, the NCSC Cyber Action Toolkit (CAT)
4. CRC members taking up Cyber Essentials/Cyber Essentials +
5. Conversion of membership to Cyber PATH services

One of the CRC Network's new strategic objectives is integration with Cross-Government SMO cyber resilience projects and initiatives; this is reflected in two of the KPIs also being NCSC priorities. The CRC Network was one of the top three amplification routes for the CAT, following its rollout in October 2025. A new performance framework and leadership structure, alongside improvements to the CRM, will enable the network to drill down into the underlying metrics, and focusing not just on headline numbers, but on demonstrating behaviour change.

A significant change for the network post-restructure, is the provision of fully-funded Cyber PATH services to SMOs (previously provided at a cost). A campaign to promote the services will commence in January 2026.

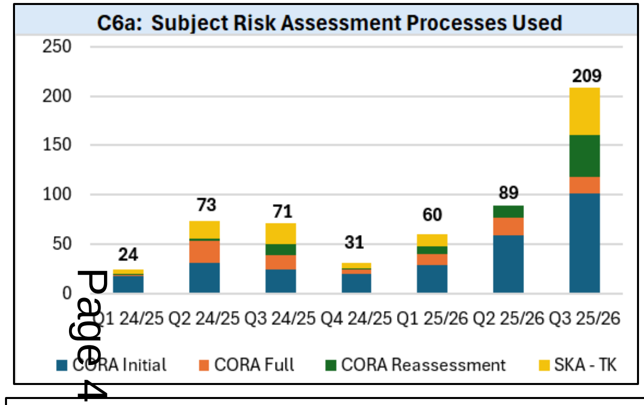
Membership as of 31st December 2025 is 29k, with 16 National Ambassadors supporting the network.

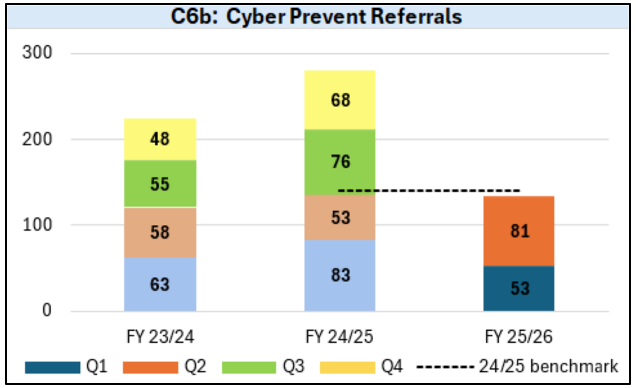
Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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 PR EVENT referrals.

FYTD	FYTD Performance	Data Trend
C6a Increase the number of CORA assessments made	🟩	⇧
C6b Increase the number of PREVENT referrals	🟨	⇨





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 Q3, risk assessments have increased by 135% (+120) in comparison to Q2 and by 194% (+138) compared to the same period for the previous year (Q3 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. A dashboard is in the process of being built to measure the impact of interventions on individuals, as a result those that are most effective in reducing risk can be identified.

C6b A total of 77 Cyber Prevent referrals were received in Q3, an 8% (-7) decrease from Q2 and a 1% increase (+1) from the same period for the previous year (Q3 24/25). Overall, Q3 is reporting 2% above the quarterly benchmark year with a total of 215 referrals for the FY 2025/25 to date.

Response

Cyber prevent teams have been reduced due to reprioritisation by the Home Office and funding reduced in 25/26. Whilst the reduction in capacity to deal with referrals reported a downturn in Q1 and Q2, referrals are now on par and have increased for Q3.

Relationships have been strengthened with Counter Terrorism (CT) and the Home Office with a formalising the roles & responsibilities for cross cutting themes. This is important as Counter Terrorism Prevent remains the network's second-largest source of referrals after schools. Formal guidance has been issued to the Cyber Prevent Network to create and standardise existing processes, ensuring Counter Terrorism and Cyber risks are appropriately managed, documented, owned and relationships clear.

Pre and post CORA interventions are now being completed to support evidence on the effectiveness of CORA and Cyber Prevent General.

The Network has had a several Prevent Managers' Governance Meetings, since September 2025, which have been chaired by the NPCC. This is to provide accountability and support to managers in relation to Prevent. This has paramount with regards to increasing the number and quality of the referrals and to share good practice.

The Network continues to run online CPD events for both managers and practitioners on the current risk and threats along with good practice. There are also opportunities for the network to attend session to get briefings from senior leaders and for them to answer questions

Deputy Commissioner Adams and DCI Catney had a meeting with Baroness Browning at the House of Lords in January 2026. Whilst the meeting was about our people in the Network, especially neurodiversity, she asked about Prevent. It was to explain how the Cybercrime Network operates and how we divert people away from cybercriminality. Baroness Browning was impressed and has asked for an additional meeting to discuss Prevent and the Cybercrime Network's people strategy.

Cyber

Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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 For Q3, there are currently 146 volunteers on Assemble, across 35 teams. The full time National Lead and Deputy Lead roles now filled, awaiting completion of vetting to start on secondment with CoLP. Formation of cadre of volunteers to work nationally in support of the Lead and Deputy Lead's strategy and delivery.

In Q3, Volunteers logged 1,189 hours of work. This is known to under-represent the true value as volunteers are not always logging their activity. A key element of the new delivery plan is to understand the barriers to recording activity and to develop a more robust way of monitoring performance. a North Wales Special Constable won the Lord Ferrer's Award for his contribution to the Cybercrime Unit and wider force, and a WMROCU volunteer came third in the Team Cyber UK Capture the Flag event.

Volunteers progressed projects to develop a network monitoring tool for domestic abuse victims, an effective radio frequency survey tool and a mapping web app. They supported CCUs at numerous protect engagements and cyber escape rooms. They undertook dark web monitoring and intelligence generation, intel analysis on money mules and cyber incidents, OSINT to secure high risk stalking victims online and progressed their own cyber work files. They supported frontline teams with ethical hacking, using Excel and understanding AI. Volunteers supported the CRC Network through business engagement, and PCA through threat report analysis and consultation around the new supplier specification.

Response

Work has started on a rebrand of Cyber Digital Specials and Volunteers (CDSV) network to reflect wider scope beyond cyber, to the Specialist Crime Volunteer Network. The team is working with the NPCC Science & Technology team and Regional Science & Innovation Managers to embed the use of volunteers within the NPCC strategy. The volunteers' skillsets and current work in the tech-facilitated abuse threat area are also of interest to the National Centre for VAWG and Public Protection.

A phased approach to the expansion of Assemble (volunteer platform) is being scoped by PA Consulting (as part of the NPCC Science & Technology in policing profession project).

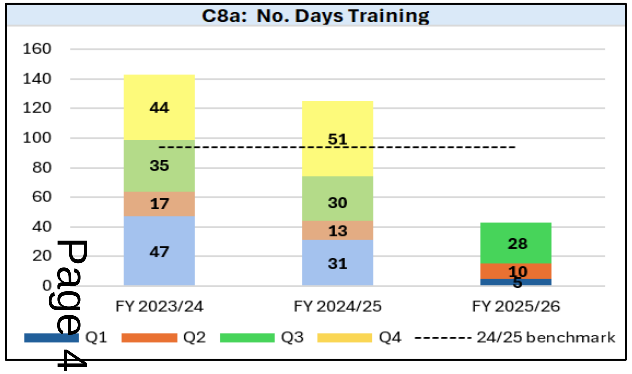
This presents an exciting opportunity for additional support/resource to the volunteering programme. A SWOT Analysis of the platform is underway, gathering user feedback and business need. PA Consulting are keen to explore the potential of piloting Corporate Volunteering, with interest currently from Lloyds Bank and the Institute of Chartered Accountants of England and Wales.

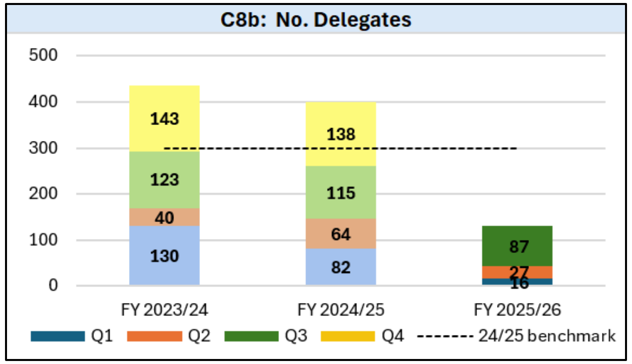
Cyber

Improve Outcomes for Victims

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	🟥	⇩





C8a For Q3, there has been a 180% increase (+18) in the number of formal training days provided in comparison to Q2. In comparison to the same quarter for the previous year (Q3 24/25), there has been a 7% decrease (-2). Q3 is reporting 38% below the benchmark (-11). Q3, although reporting below the benchmark, delegates and training days have both reported large increased in comparison to Q1 & Q2.

C8b During Q3, 87 delegates were delivered formal training courses, this is a 222% increase (+60) in comparison to Q2 and a 24% decrease (-28) when compared to the same period for the previous year (Q3 24/25). Overall, Q3 is reporting 57% under the benchmark (-169).

Sudocyber	Labs Completed
Oct-25	524
Nov-25	334
Dec-25	552
Total	**1,410**

Response

There was a delay in the implementation of the training programme due to the budget not being finalised by the Home Office for Q1, it was started during Q2, before maximising the number and range of courses in Q3/Q4.

It was decided that courses would be released for the entire year rather than quarterly as previously done. This allows managers in the network to be more flexible with their budgets and when staff attend. The courses have also been delivered (where appropriate) in the North of the country.

A cyber incident response course was developed with the training provider and the NPCC. The course is tailored for the police and allowed practitioners and managers (SIOs) to take part on the same course, but learning their role in an incident. Both groups would be brought together at regular intervals to enhance the learning. This provided staff with the skills and knowledge, whilst at a more cost-effective price than outsourcing it. The feedback has been positive and is now part of the suite of national courses offered.

The NPCC is running a tendering process for training courses for 2026/27 and beyond.

SudoCyber has been running a Capture the Flag (CTF) Exercise in partnership with the NPCC to engage better with the users in the cybercrime network. This resulted in a grand final in Cardiff. SudoCyber will be putting on additional CPD events in 2026.

This page is intentionally left blank

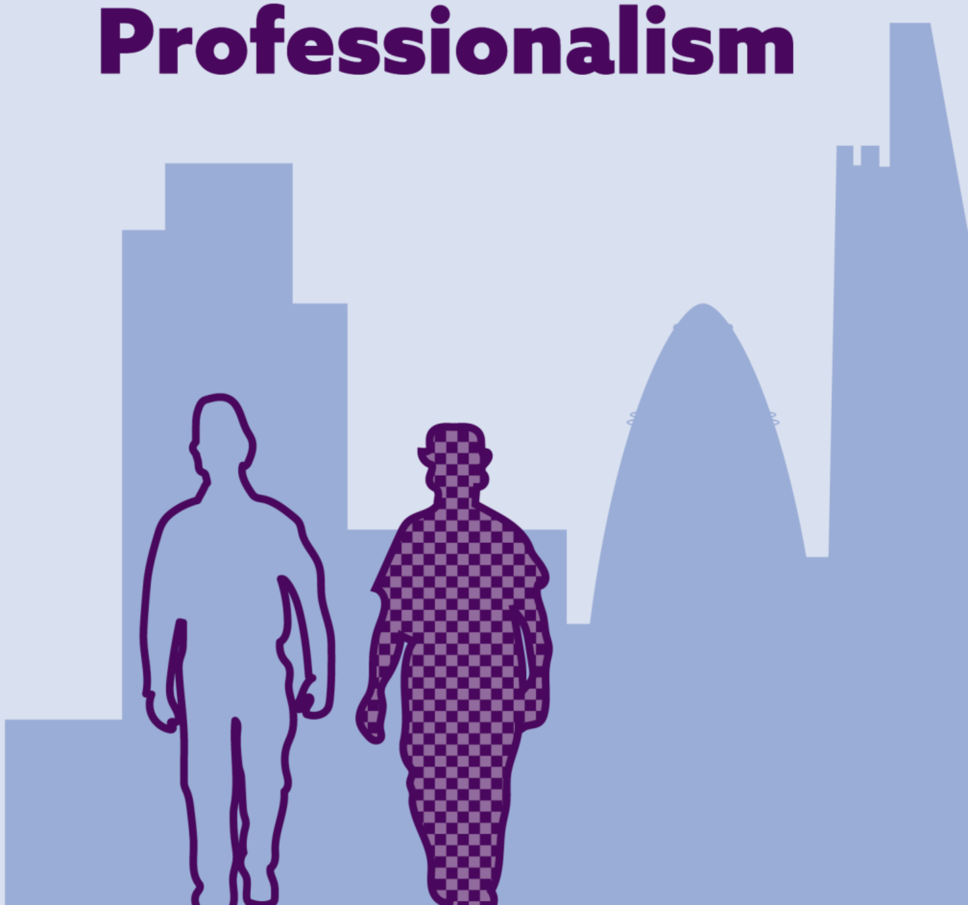
CITY OF LONDON

CITY OF LONDON POLICE

Integrity
Compassion
Professionalism

Policing Plan Performance

Quarter 3 2025/26



Background –Summary performance

Policing Plan Performance Measure	Committee oversight	Quarterly Performance	Data Trend
Reduce Theft	Local Policing Committee		
Respond Effectively to Theft	Local Policing Committee		
Reduce Violence	Local Policing Committee		
Respond Effectively to Violence	Local Policing Committee		
Protect the City from Terrorism	Local Policing Committee		
Victim Satisfaction	Local Policing Committee		
Case Compliance with Victims Code of Practice	Local Policing Committee		
Implement victim-focussed commitments from our fraud, economic and cyber crime strategy	Economic, Security and Cyber Crime Committee	Unavailable	
Secure positive outcomes for victims of crime in the City	Local Policing Committee		
Protect people and businesses from economic and cyber crime	Economic, Security and Cyber Crime Committee	🟧	Narrative
Narrative assessment on the status of the Fraud and Cyber Crime Reporting and Analysis Service programme	Economic, Security and Cyber Crime Committee	🟧	Narrative
Narrative assessment of the results of national fraud intensifications and intelligence led operations	Economic, Security and Cyber Crime Committee	🟩	Narrative
Increase positive outcomes for reported fraud and cyber crime nationally and locally	Economic, Security and Cyber Crime Committee	Unavailable	
Narrative assessment of progress against the EDI strategy implementation plan	Professionalism & Trust Committee		
Narrative assessment of engagement activity across the City	Local Policing Committee		
Assessment of complaint handling quality via Professional Standards and Integrity Committee dip check of cases	Professionalism and trust committee		
Public confidence in the City of London Police is increased	Professionalism and trust committee		
Maintain our officer uplift commitment	Resources and Estates Committee		
Achieve and maintain at least 90% of our police staff permanent establishment	Resources and estates committee		
Narrative assessment on action taken to attract, recruit and retain the best talent	Resources and Estates Committee		
Maintain or increase Crime Data Integrity standards	Local Policing Committee		
Increase workforce engagement with our self-service data dashboard	Local Policing Committee		
Financial outturn is within 1% of forecast	Resources and Estates Committee		
Narrative assessment on the progress of the productivity action plan	Resources and Estates Committee		

Put victims at the heart of everything we do

Implement victim-focussed commitments from our fraud, economic and cyber crime strategy

Data Trend	

Reduce number of repeat victims of fraud

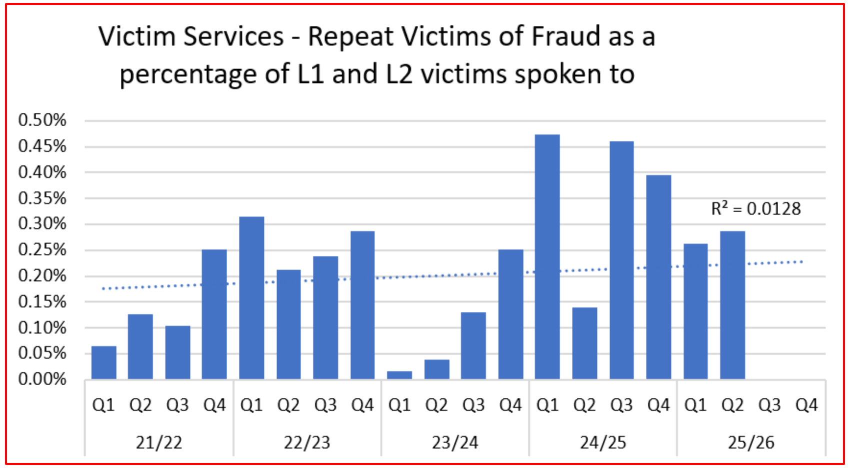
The **Report Fraud Victim Services Unit** supports forces at a local level, delivering care to victims of fraud and cyber-crime, allowing for a consistent and national standard of care and support. The **Level 1** service gives Protect/Prevent advice to non-vulnerable victims of fraud. The **Level 2** service engages with victims when vulnerability is identified, and by giving crime prevention advice and signposting to local support services helps the victim to cope and recover from the fraud.

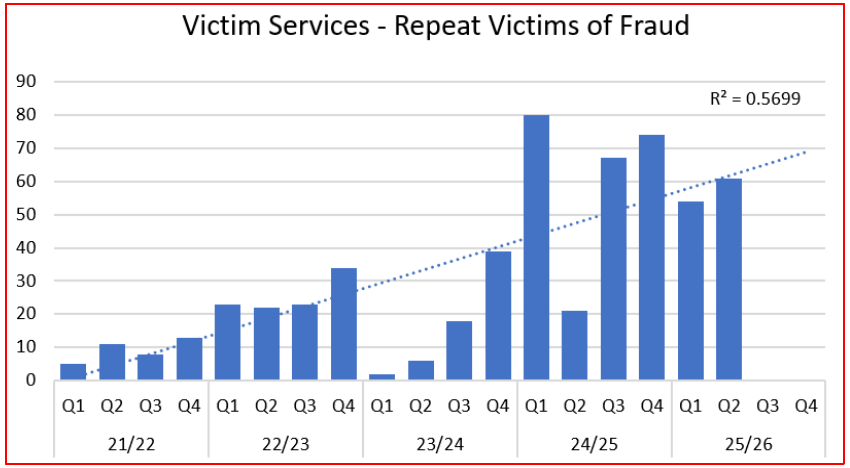
The definition of a repeat victim is “a second or subsequent report by a victim of fraud who has had previous contact with Victim Services within a rolling 12-month period”.

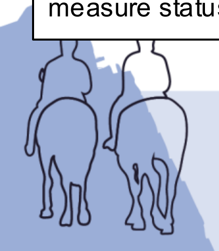
The delivery of Report Fraud Reporting Analysis and Victim Services went live on 4th December 2025 with a public launch on 19th January 2026. The data platforms and reporting processes are still being refined and it has not been possible to provide like for like information to be reported on for this performance product.

However, the early performance reporting from the system for December 2025 has been provided as an appendix, as an early insight to how the system and processes are performing and CoLP is confident the data position will be improved in the coming weeks ahead of Q4 reporting.

Please note no Q3 data is included and therefore success measure status has not been included.







Improve the national policing response to fraud, economic and cyber crime

Protect people and businesses from economic and cyber crime

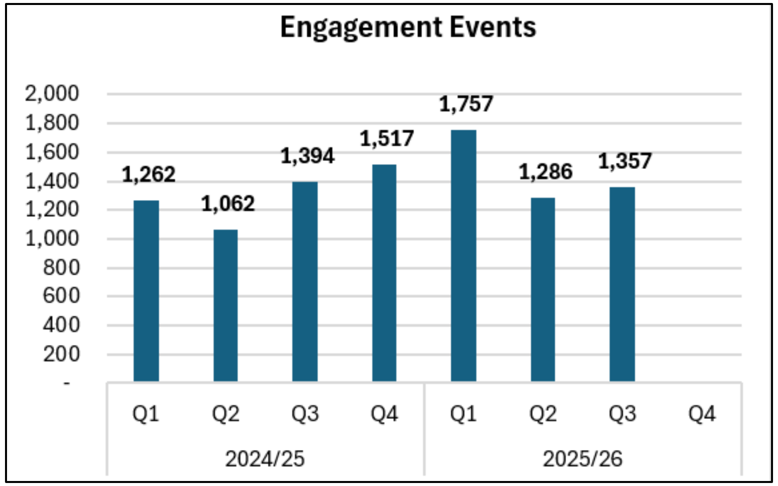
Data Trend ➡

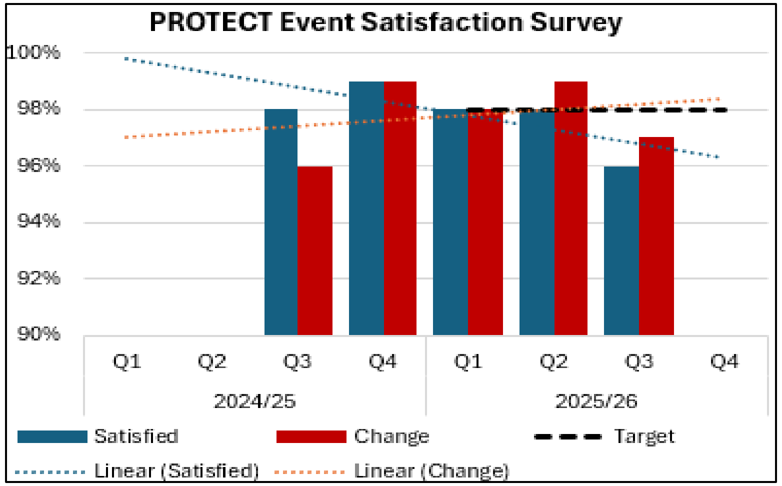
Percentage of PROTECT engagement event attendees (organisations and public) likely to change their behaviours as a result of the event.

For Q3, 1,357 engagement events were recorded under the fraud and cyber protect response type this quarter. This is a 6% increase (+71) in comparison to Q2 25/26 and a 3% decrease in comparison to the same quarter for the previous year Q3 24/25 (-37).

Protect engagement events are reporting 8% (+325) above the quarterly benchmark for this year.

This quarter 96% of attendees were either very satisfied or satisfied with the event, this is a 2% decrease from Q2. Additionally, 97% were likely to change their behaviour as a direct result of the event, this is a 2% decrease from Q2. The figures show a slight decrease in positive response towards audience behaviour change for Q3.





Response

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. The National Lead for Protect and the Home Office have emphasised to the Regional Coordinators how important they are. Staff consistently receive high praise from attendees for the quality of information shared, and their delivery.

In Q3, as part of Op Tonic, Report Fraud Protect Services coordinated a partnership with Barclays who have a fleet of vans that go to various locations to provide banking services to the community, these also offer mobile fraud awareness sessions. During the romance fraud intensification week, several protect officers from various regions joined the Barclays staff in the vans to promote romance fraud awareness (as well as general fraud awareness).

In October, for Cyber Security Awareness month, the Protect team focused on promotion of a video in partnership with Meta on 2 Step Verification. The social media campaign reached over 300,000 people with 637,904 impressions.

The Online Shopping Campaign launched on 24 November to help the public to shop safely online. This campaign was done in partnership with the National Cyber Security Centre and Stop Think Fraud. The Online Shopping Campaign reached over 1.7 million people across the UK with 2.8 million impressions. The social media assets were used 114 times by partners and polices forces.
As part the Action Fraud organic reached the Online Shopping Campaign had over 300,000 impressions and 2,000 reactions across Instagram, Facebook and X.

Projects for Q4:

For Q4, the Protect team will be collaborating with SWROCU with a focus on proactive romance fraud and victim protect notifications. The process and policy documents are currently being created and reviewed prior to the operation start.

A trusted and inclusive police service, keeping the City of London safe and transforming the national policing response to fraud, economic and cyber crime

Status of the Fraud and Cyber Crime Reporting and Analysis Service programme

Assessment of the status of the Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) programme

Overview:

The City of London Police, through the FCCRAS programme, is delivering the replacement service for the underperforming Action Fraud; a critical component of the Fraud Strategy. The new service will deliver much-enhanced reporting and analytical services which align with the strategic aims of HMG's Fraud Strategy (cutting fraud) and the National Cumber Strategy (building resilience).

Programme Deliverables:

FCCRAS will deliver a new national reporting service that offers improved reporting tools and support services for victims, better intelligence to policing for investigations, and allows for greater prevention and disruption at scale.

Key Delivery Dates:

Following approval of a revised business case including funding and new detailed implementation plan, the programme has been working to the following timeline for implementation of the new service:

- Public Beta: 11 November 2025
- Full-Service Go Live: 04 December 2025
- Campaign Launch: 19 January 2025

Delivery Status:

The FCCRAS programme shifted from reporting Amber to 'GREEN' in Q3 of FY 25/26 due to the successful delivery of the new Report Fraud Service.

Report Fraud Service Delivery

- *Public Beta*: on Tuesday 11 November, the FCCRAS Programme completed the phased launch of the Report Fraud Service, entering 'Public Beta'. This saw the service run in parallel with the legacy system for 4-weeks, enabling the contact centre call handlers to be trained in cohorts, and the integration between the online reporting tool, N-VRS (Victim Relationship System) and N-CAS (Crime Analysts System) to be tested in real time. This allowed the product team to refine defects and iron out any issues ahead of the full-service launch.
- *Full Service Go Live*: on Thursday 04 December, the Report Fraud Service went full live, building on the successful launch of Public Beta. This meant all internal and public facing systems are now operational, including website and new brand.

NISTA Gateway 4

- FCCRAS underwent a 5-day review of the programme between Monday 27 and Friday 31 October. The NISTA review assessed FCCRAS delivery confidence as AMBER. The review team did not identify any blockers to a 'go' recommendation for the full service go live, noting there was a high level of confidence in the new service and underpinning technology, however several risks were identified in relation to operational readiness.
- The review commended several areas of good practice such as commercial strategy and management, financial planning, and knowledge management. They made ten recommendations, five of which were critical, and an action plan has been scoped to commence mitigations against each risk and ensure the service is in a strong position for BAU.

FCCRAS Workstreams

To support the new service being launched, significant progress was achieved across the 17 workstreams in the programme. A few highlights include:

- *Commercials*: Following negotiations, an uplift in the 2025/26 FY was agreed with the Home Office and City of London Corporation. This has also been approved via InvestCo and HMT, increasing the WLC of the programme. All schedules in the Lot 1 contract were agreed and signed between CoLP and PwC
- *Accreditation*: the Report Fraud service has received National Accreditation by the National-SIRO (PDS led)
- *Decommissioning*: the incumbent supplier of the legacy system – IBM – have now disabled the front-gateway and user access to the old platforms. All data from IBM has been migrated, validated and ingested into the new service.
- *Interoperability*: the service has onboarded early adopters to the generic search functionality; Op Recall has been rolled out with further enrolment planned for early 2026
- *Content Management*: all content for the new service has been QAd and updated to the new systems, this includes protect advice, website, social media, chatbot, etc.

Planned Activity for Q4

- Engagement with NISTA and Home Office to plot out the Gateway 5 for FCCRAS
- Preparation of programme closure documentation, including lessons learnt, transition from programme to BAU
- Brand and Campaign Launch in January 2026
- Deployment of the PND integration
- Closure of accreditation risks

Assessment of national fraud intensifications and intelligence led operations.

Results of national fraud intensifications and intelligence led operations:

Op Callback 2

In Q3, Op Callback 2 took place; this was an 8-week intensification focusing on Courier Faud which is a form of deception in which offenders impersonate trusted authorities to manipulate victims into handing over valuable items to a courier. This was a joint operation working alongside the Metropolitan Police. Currently data is being analysed but the Metropolitan Police have reported 33 arrests, 9 charges, 61 serious and organised crime disruptions and £55,000 in cash seized.

This intensification also provided links to two other on-going operations involved in courier fraud, identifying two distinct modus operandi involving courier fraud.

Op Tonic took place from 29th September – 5th October. This was a one-week Romance Fraud intensification initiative for “World Romance Fraud Scam Prevention Day” on the 3rd October 2025. The primary aim was to raise awareness, deliver protect advice and encourage reporting of romance fraud. This also involved collaboration and joint working with Barclays fraud and scam vans in engagement days. This intensification reported 2,299 posters distributed nationally, 12 engagement days, 61,142 impressions recorded on Facebook by Report Fraud and 405,516 social media impressions reported from forces. Overall given the short timescale and limited resources, the fraud network pulled together collaboratively to promote romance fraud awareness on a national level. They delivered some great events and engaged with the public successfully.

DO YOU REALLY KNOW WHO YOU'RE TALKING TO?
ROMANCE FRAUD IS ON THE RISE
STOP! THINK FRAUD
CITY OF LONDON POLICE

Op Tonic engagement poster

Upcoming intensification

Op Henhouse 5

City of London Police are working with the National Economic Crime Centre to deliver Henhouse 5 in February 2026. This will see coordinated pursue and protect activity across all 43 police forces, PSNI, Police Scotland, every regional organised crime unit, Trading Standards, FCA and NCA, SFO and Insolvency Service.

Increase positive outcomes for reported fraud and cyber crime nationally and locally

Data Trend

Increase positive outcomes for reported fraud and cyber crime nationally and locally

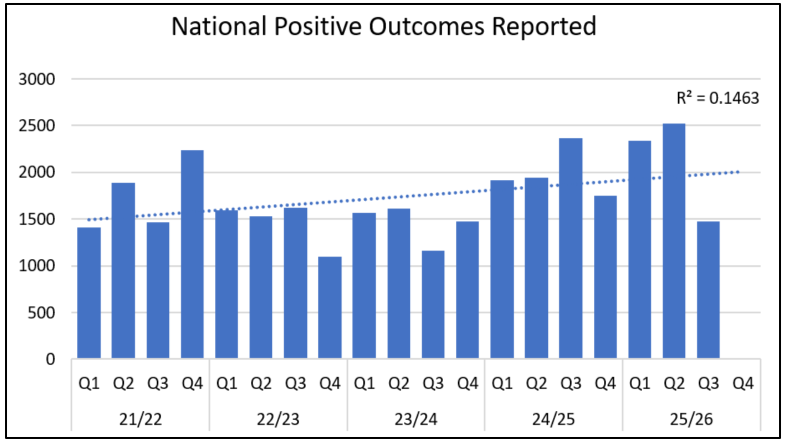
Nationally the positive trend has continued through Q3, but at a slowing rate, with **1,478** positive outcomes, compared to Q1 2,341 and Q2 2,541.

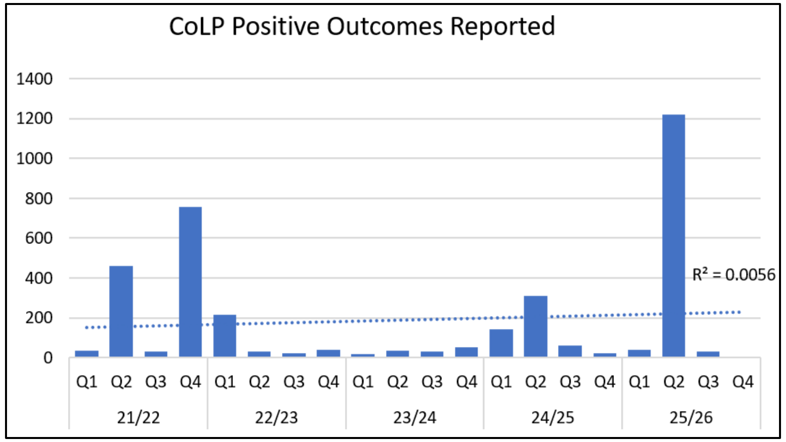
Against the comparative period last year positive outcomes for Q3 were down by 38%, (-889). This is due to Q3 25/26 not containing any large one-off cases from forces, thus averaging circa 500 per month (i.e. a run rate of circa 6,000 per annum). For the year to date 9 months to 31st December 2025, total positive outcomes were **6,340**, up **122 (+2%)** on the prior year.

Key drivers across the first 9-month period include an Investment Fraud operation from NLF CoLP yielding 1,199 outcomes in September. Q1 reflected strong monthly returns from many forces, in combination with large returns from two forces; a Ponzi scheme and a large return for an Abuse of Position Fraud from one, and a Retail Fraud from the other. These totalled more than 350 outcomes each in one month.

Total CoLP positive outcomes across all units remain flat with circa 11 returns a month on average, excluding large one-off operations. However, the pipeline remains strong.

Positive Outcomes have been calculated using the legacy systems rather than the new National Crime Analysis System (NCAS) this quarter. Analysts are working on the reporting of outcomes recorded in NCAS and these will be added to legacy outcomes from Q4 which may increase Q3 totals.





Response

On 14th October 2025 a Fraud Lunch and Learn Session was hosted by Commander Garnett. All Chief Officer Teams from across the country were invited to the virtual event which was well received. The content of the event was matched closely to the key elements of advice being shared with forces through NCO engagement.

In Q3 25/26, the NCO visited and supported 15 forces, with a further 3 booked already for Q4. These visits are predicated around direct requests for support in anticipation of forthcoming HMICFRS visits (excluding Police Scotland and BTP). However, the NCO are not seeking to coach or mentor forces through those inspections but are providing forces with advice and guidance to good practice when formulating a response to fraud.

Q3 for CoLP reflected a return to BAU volumes of positive outcomes in line with Q1. In Q2, NLF CoLP recorded an Investment Fraud which yielded 1,199 positive outcomes. There are a number of ongoing investigations of Investment Frauds within CoLP, which are young and at a pre-charge stage, and all hold significant volumes of victims.

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. For example, one investigation into a boiler room might have hundreds of outcomes attached to it and closing the case will give many outcomes, potentially bringing closure to multiple victims.

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee – for information	**Dated:** 23 February 2026
Subject: NLF Performance Framework refresh.	**Public report:** For information
This proposal: • **delivers Corporate Plan 2024-29 outcomes**	City of London Policing Plan
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:	Commander Tor Garnett
Report author:	T/Chief Inspector Megan Cardy

Summary

This paper proposes new a refresh of the performance framework metrics for City of London Police's national leadership functions, to ensure they are fit for today, that accountability is clear and that we have a greater balance of quantitative achievements to point to regarding the impact of our national leadership functions. The paper sets out proposed revisions under two of the six pillars of our Policing Plan 2025-28 Performance Framework for ESCCC discussion.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. City of London Police has undertaken a review of performance measures for its national leadership functions to ensure they are fit for today, that accountability is clear and that we have a greater balance of quantitative achievements to point to regarding the impact of these functions. The aims of the review were to:

   - Bring together a single NF Performance Framework as opposed to separate disconnected but overlapping performance frameworks (eg ESCCC, Home Office, NECC Governance, Report Fraud Benefits Framework)
   - Ensure each external and internal customer gets what they need to drive accountability
   - Join up tactical performance focus with strategic performance focus across all economic fraud anc cyber crime workstreams.
   - Continuously improve our data accuracy, literacy and visualisation

Current Position

2. For the 2026 Refresh of the CoLP Policing Plan the Chief Officer team have agreed the following updates to the Policing Plan Performance Measures under the following two categories overseen by ESCCC:

   - Policing Plan Priority 2: *Put victims at the heart of everything we do*
   - Policing Plan Priority 3: *Transform the national policing response to fraud, economic and cyber crime*

3. A wider NLF Performance Framework with a suite of monitoring measures sitting below this, which will inform the narrative and actions taken to address performance concerns or support improvements, is yet to be finalised.

4. Draft proposals will be presented to Police Authority Board on 25th February as part of the Policing Plan refresh paper. Feedback is sought be ESCCC members in in advance of this meeting.

Proposals

Policing Plan Priority 3: Transform the national policing response to fraud, economic and cyber crime

5. Move from the current Policing Plan NLF headline measures:

   1) **Protect -** The % of protect engagement event attendees likely to change their behaviours as a result of the event
   2) **Reactive Pursue -** Increase Judicial Outcomes for Reported Fraud and Cyber Crime nationally and locally
   3) **‘Narrative only’** - Status of FCCRAS

4) **‘Narrative only’** - Results of the 4 National Fraud Intensifications + intel led ops
5) **Not reported on currently -** Increase the number of Frauds Avoided (we can’t do it internally as it requires an economist to administrate effectively)

6. To the following headline measures from April 2026 onwards:

1) **Crime Reduction -** At least a 10% reduction in average loss for Policing Control Strategy Fraud types – Abuse of Position, Courier Fraud, Romance Fraud (UK based), Investment Fraud. (using median for a rolling 12 month as this fluctuates significantly). *To be Reported Quarterly.*
2) **Proactive Pursue -** At least a 10% increase in total national value receipted from successful Asset Recovery proceedings. (success measure should be considered as a rolling 12 month as this fluctuates significantly). However acknowledging there is low confidence in data until ARIT is delivered). *To be Reported Quarterly.*
3) **Stop + Block Cyber/Fraud Disruption -** At least a 1000% increase in the volume of instances where data sharing leads to offenders being stopped or blocked (i.e. removal of tech or finance identifiers enabling fraud). *To be Reported Quarterly.*
4) **‘Traditional’ Cyber/Fraud Protect -** At least a 20% increase in the number of CRC businesses in membership and a 500% increase in the national brand partnership reach figures. *To be Reported Quarterly*
5) **National Leadership Quality –** Increasing national productivity – positive outcomes (CJ + disruptions) per 100 hrs of demand (volume of proactive + reactive disseminations) put into the policing network. *To be reported as a deep dive report by Q3 2026/27 and annually thereafter.*

Policing Plan Priority 2: Put victims at the heart of everything we do

7. Move from the current Policing Plan NLF headline measure:

1) **Repeat Victimisation -** Reduce the number of repeat victims of Fraud (currently only report those who go through NEVCU, trying to move to data as a % of all reported victims, however the significant volume of underreporting undermines this measures value)

8. To the following headline measures from April 2026 onwards:

1) **Public Trust + Confidence -** A reduction in the gap between Report Fraud reports and CSEW estimates from 89% of crime estimated to be unreported to 85% across the 3 year period. *To be Reported Quarterly*
2) **Reactive Pursue -** Increase in Positive Outcome rate for Reported Fraud nationally and locally (At least a 5% increase across the 3 year period

acknowledging the lag between Report Fraud and complex fraud investigations reaching CJ Outcome), (in line with agreed police outcome reporting agreed by NPCC, HO and HMICFRS). *To be Reported Quarterly*

3) **Local performance in managing risk and serving the public -** An increase in the proportion of forces achieve HMIC Outstanding, Good or Adequate (baseline from January 2026 when first moderated gradings will be released). *To be Reported Bi-annually.*

Corporate & Strategic Implications

Strategic implications – The content of this paper contributes to delivery and measurements of our Policing Plan priorities (which also contributes to the delivery of Corporate Plan objectives).

Financial implications - n/a

Resource implications – n/a

Legal implications – n/a

Risk implications – n/a

Equalities implications – measuring trust and confidence through the Crime Survey for England and Wales should enable us to understand how these rates differ by protected characteristics.

Climate implications – n/a

Security implications – n/a

Appendices

None

Megan Cardy
Head of Performance and Strategic Insights
E: megan.cardy@cityoflondon.police.uk

City of London Corporation Committee Report

Committee(s): Economic Security and Cyber Crime Committee (ECCC)	**Dated:** 23 February 2026
Subject: Summary of Action Fraud public complaints data – Q3 2025/26	**Public report:** For Information
This proposal: • 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 Tom Hill

Summary

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

Action Fraud changed to Report Fraud during Q3. Professional Standards are unable to amend the national complaint database (Centurion) to reflect the name change. However, the IOPC has been made aware of the change.

A total of 93 complaint cases were logged in Q3 2025/26. This is an overall decrease of 38 cases from Q2 2025/26 (29%). Schedule 3 complaints reduced from 6 to 1 (83%) from the previous quarter. Non-Schedule 3 complaints reduced by 26% to 92, and allegations decreased by 18% to 108. The average number of allegations for Q3 is below the five-quarter average of 124. The most common allegation category

was "Police action following contact" (64), followed by "General level of service" (24) this was largely driven by unmet expectations regarding Report Fraud investigations.

Complaint finalisations reduced marginally from 96 to 91 (5%), with Schedule 3 finalisations decreasing by 74% (7 cases, from 27 in Q2). Non-Schedule 3 finalisations increased by 22%, from 69 in Q2 to 84 in Q3. The average time to finalise all complaints was 243 days, based on retrospective IOPC bulletins.

Comparison data in relation to Action Fraud reports is no longer available due to the change in service to Report Fraud.

Recommendation(s)

Members are asked to:

Note the report.

Appendices

- Appendix 1 – Summary of Action Fraud public complaints data– Q3 2025/26

Tom Hill
Detective Superintendent Tom Hill
Head of Professional Standards

T: 07803305003
E: thomas.hill@cityoflondon.police.uk

	Summary of Action Fraud public complaints data– Q3 2025/26			
Metric	**Current quarter (Q3)**	**Previous quarter (Q2)**	**(%) change (Q on Q)**	**Comment**
Complaints – Schedule 3	**1**	**6**	**-83%**	A total of 93 cases were logged in Q3 2025/26. This is an overall decrease of 38 cases from Q2 2025/26 (29%) The average number of cases logged over the previous 5 quarters is 114 per quarter, Q3 is below average. AF changed to RF during Q3. This will be a period of change and PSD are unable to amend the Centurion complaint database to reflect the name change. The IOPC have been made aware of the name change.
Complaints – not Schedule 3	**92**	**125**	**-26%**	
Allegations	**108**	**131**	**-18%**	There were 108 allegations recorded in Q3 2025/26. This is a decrease of 23 allegations from Q2 2025/26 (18%). The average number of allegations over the previous 5 quarters is 124 per quarter. Q3 is below average.
Average time to log complaints (days)	**N/K**	**5**	**-**	*Timeliness is taken from IOPC published bulletins and available retrospectively, unavailable dataset from Centurion.*
Average time to contact complainant (days)	**N/K**	**2**	**-**	
Complaints finalised – Schedule 3	**7**	**27**	**-74%**	A total of 91 cases were finalised in Q3 2025/26. This is an overall decrease of 5 cases from Q2 2025/26 (5%) Average number of total cases finalised is 88 over the last 5 quarters. Q3 is therefore above average.
Complaints finalised - not Schedule 3	**84**	**69**	**22%**	
Average time to finalise complaint cases (days) – Schedule 3	**243 average combined data**	**243**	**n/a**	*Timeliness is taken from IOPC published bulletins and available retrospectively.* *Quarter Case combined data average 243 days (ex subjudice) from Centurion for Q3 finalised. See graph.* *IOPC bulletin will publish breakdown by case type logged (YTD – Q2 therefore average of the yearly data)*
Average time to finalise complaint cases (days) – not Schedule 3		**185**	**n/a**	
Applications for review sent to local policing body	**0**	**1**	**0**	None recorded during Q3
Applications for review sent to IOPC	**0**	**1**	**0**	None recorded during Q3

Nature of allegations – Of the 108 allegations recorded during Q3 2025/26 the highest number was in the category of, A1 – Police action following contact (64) followed by General level of Service (24) Reasons for complaint mostly relate to customer expectation of Action Fraud, with either the lack of contact or investigation cited. This is a decrease in allegations recorded against Q2 of 23 (18%).

Members of Parliament –

There have been 36 miscellaneous cases logged where MPs have contacted PSD on behalf of a constituent. This is a decrease of 69 against the previous quarter. The average being logged as 64 over the last 5 quarters.

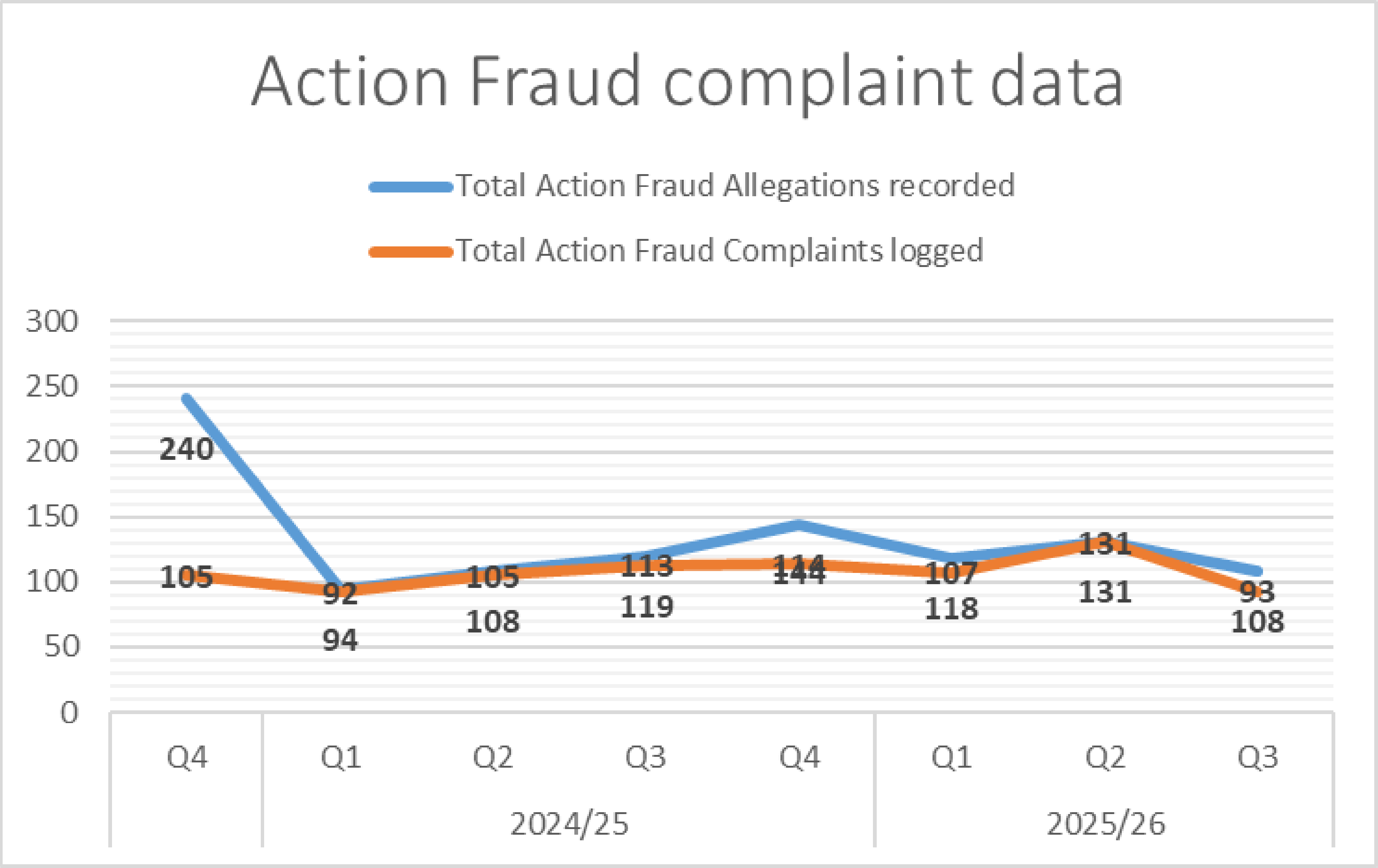
Action Fraud – comparison data is no longer available due to the change in service to Report Fraud. Last update below for Q2.

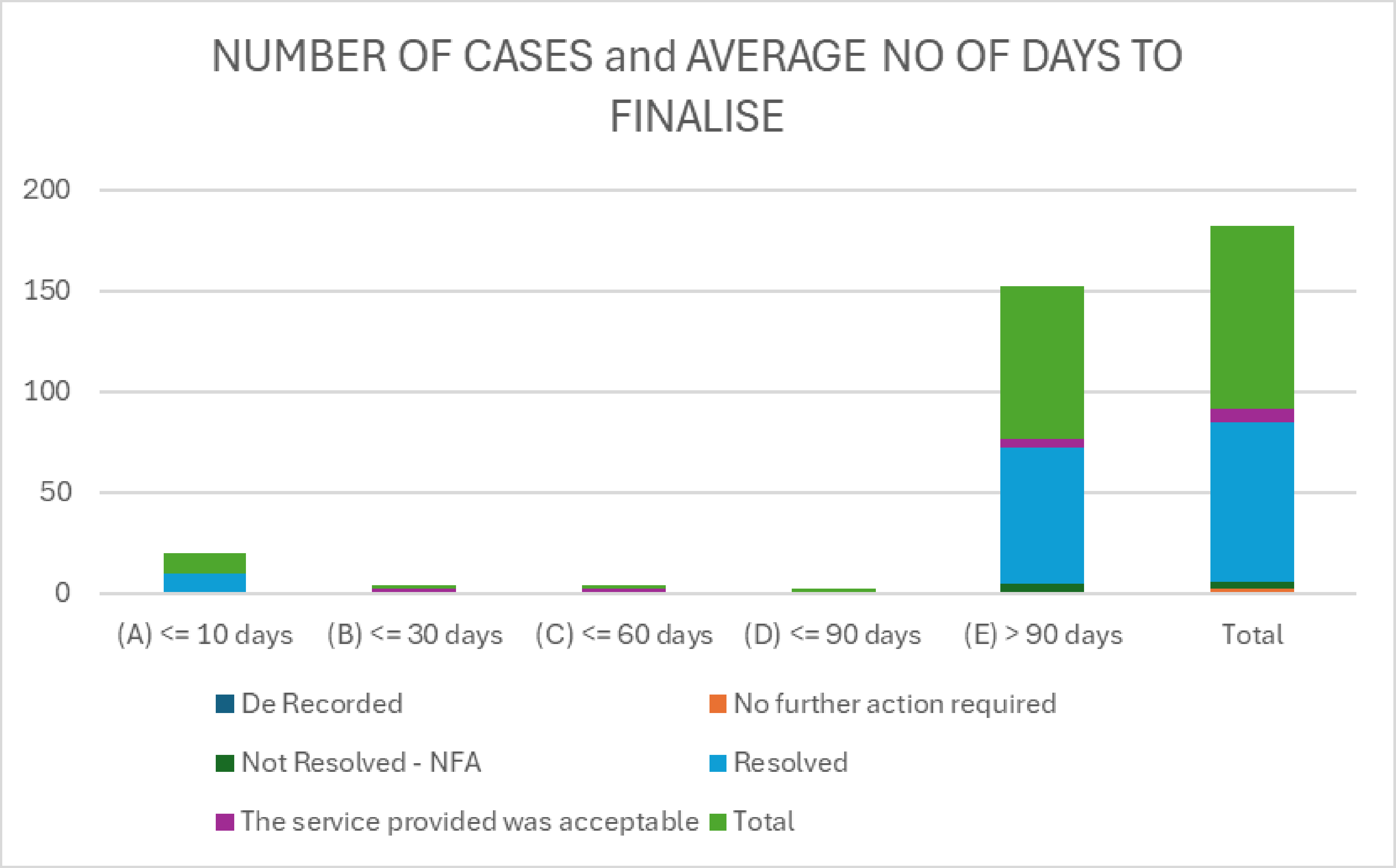
In **QTR 2** of the 2025/26 Financial Year Action Fraud recorded **147,394** reports on the National Fraud Database (Increase 10% v QTR 1)
In **QTR 2** of the 2025/26 Financial Year Action Fraud recorded **113,613** crime reports (Increase 13% v QTR 1), and **48,300** Information reports (Increase 4% 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, uncleansed 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.


Action Fraud complaint data
Total Action Fraud Allegations recorded
Total Action Fraud Complaints logged
300
250
200
150
100
50
0
240
105
92
94
105
108
113
119
114
144
107
118
131
131
93
108
Q4
Q1
Q2
Q3
Q4
Q1
Q2
Q3
2024/25
2025/26


NUMBER OF CASES and AVERAGE NO OF DAYS TO FINALISE
200
150
100
50
0
(A) <= 10 days
(B) <= 30 days
(C) <= 60 days
(D) <= 90 days
(E) > 90 days
Total
De Recorded
No further action required
Not Resolved - NFA
Resolved
The service provided was acceptable
Total

Agenda Item 9

City of London Corporation Committee Report

Committee(s): Economic & Cyber Crime Committee	**Dated:** 23/02/2026
Subject: Cyber Resilience Centre (CRC) Network Update	**Public report:** For Information
This proposal: Updates member on the closure of regional CRCs as private businesses and future direction	Supports the CoLP Policing Plan
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£0
What is the source of Funding?	N//A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	Deputy Commissioner Nik Adams
Report author:	Detective Chief Supt Andrew Gould

Summary

This report updates members on the closure of regional Cyber Resilience Centres (CRC) as private businesses and transfer of assets and staff to City of London Police and the National Cyber Resilience Centre Group, owned by the Corporation. It also outlines the new CRC Network Strategy and Delivery Plan.

Recommendation(s)

Members are asked to:

- Note the report.

Main Report

Background

1. The Cyber Resilience Centre Network is a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the sole trader, micro, small, medium business and third sector communities, as a key part of HM Government's National Cyber Strategy and the NPCC Cybercrime Plan. A key focus for the network is to secure supply chains and to protect the UK economy.

2. Small and medium-sized enterprises (SMEs) accounted for 99.9% of the UK business population at the start of 2024, with 99.2% being small businesses with fewer than 50 employees. SMEs make up the vast majority of the UK's supply chains. Smaller organisations typically lack in-house expertise and may never have benefited from cyber resilience advice, due to a lack of awareness of cyber threats, prohibitive costs, or not knowing where to start and who to ask for help.

3. The CRC Network proactively identifies ways to reach SMEs to provide cyber security guidance, raising awareness and encouraging behaviour change to drive cyber hygiene. The CRC Network promotes and aligns with services, products and guidance from the National Cyber Security Centre (NCSC). The network is *"Police Led, Business Focused"*, capitalising on policing being a trusted source of crime prevention advice, in what is recognised as a cluttered and confusing market.

4. The CRC Network provides long-term guidance, through a customer journey model, involving regular, engaging bitesize cyber security advice to members, tailored to specific regions or sectors. The journey aims to develop understanding over time. The primary aim of our student services **Cyber PATH** is to provide SMEs with fully funded cyber security services, from a trusted source, to improve their risk awareness, hopefully resulting in improved cyber resilience and onward referral to Cyber Essentials (CE) partners or CE certification.

5. There were a number of challenges that made the current operating structure untenable. These included:

- Risk of non-compliance with competition, subsidy and data sharing laws and regulation.
- Barriers to full support and public engagement by the National Cyber Security Centre (NCSC).
- Home Office, alongside NCSC and Dept Science, Innovation and Technology (DSIT), ambitions to significantly build on the regional delivery model with CRCs acting as the focal point for HMG interventions, requiring greater flexibility and accountability to central government.

- Inability to deliver sufficient effective National Police chiefs Council (NPCC) leadership and governance across the CRCs as private limited companies to ensure appropriate minimum standards and assurance required for National Cyber Security Centre (NCSC) and Home Office support.

6. A decision was made that:

1. The regional CRCs would close as businesses and be fully integrated into policing;

2. CRC staff would be line managed and led nationally from CoLP but maintain local and regional delivery through the Regional Organised Crime Units.

3. Assets and privately employed staff would transfer to the National Cyber Resilience Centre Group (NCRCG), owned by the Corporation.

Current Position

7. Expert support was engaged from Pinsent Masons and RSM to advise and assist with the transfer of CRC assets and staff. Ownership of the regional CRC companies transferred to NCRCG for voluntary liquidation to be undertaken by RSM. Transition proved to be significantly more challenging and complex than envisaged with a number of local corporate governance and other issues requiring resolution prior to transfer. These have all been resolved and all assets and staff from Wales, London, South East, Eastern, East Midlands, West Midlands, North East and North West CRCs transferred before Christmas. The South West has been delayed by staffing issues which have now been resolved and transfer is imminent. All police officers and staff seconded to their CRCs have now been seconded to City of London Police. A new network operating model was developed and delivered, is now in place and working well.

8. Last year saw a substantial increase in funding for the CRC Network from the government's Integrated Security Fund. This has funded the transition and replace previous regional private sector contributions. Going forward, we have been informed by the Home Office there may a further increase to improve our current capacity and capability, help grow our messaging and help us scale. We continue to take financial contributions from our National Ambassadors via NCRCG.

9. This will be a year of transition for the CRC Network as we move from CRCs being private businesses to being wholly controlled by policing. We are committed to embedding the new operating structure, supporting national and regional stakeholders, delivering growth in membership and service delivery. Alongside this, we have agreed CRC Network priorities and objectives with the Home Office and National Cyber Security Centre, which will focus on the following:

- Managed Service Providers for SMEs

- Small & Medium Sized Enterprises holding large personal datasets
- Supporting existing CRC members
- Closer alignment with National, Regional and Local Cyber Protect teams
- Integration with cross-government projects on SME resilience
- Growing membership, primarily through National Ambassador and large organisation campaigns across their SME customers and supply chains
- Promotion of Cyber Essentials

Options

10. None.

Proposals

11. None.

Key Data

12. CRC Network membership has grown to 29,000 across England & Wales. A performance framework is under development with the Home Office and NCSC focused on key outcomes and behaviour change including Cyber Essentials uptake.

Corporate & Strategic Implications

Strategic implications

13. Supports the CoLP Policing Plan.

Financial implications

14. None.

Resource implications

15. None.

Legal implications

16. None.

Risk implications

17. None.

Equalities implications

18. None.

Climate implications

19. None.

Security implications

20. None.

Conclusion

21. The closure of regional Cyber Resilience Centres (CRC) as private businesses and transfer of assets and staff is largely complete. This is now enabling a more consistent, high quality service to be delivered. This consistency and the new operating model will enable the large scale growth of membership and support to SMEs required to support cyber resilience in SMEs at scale.

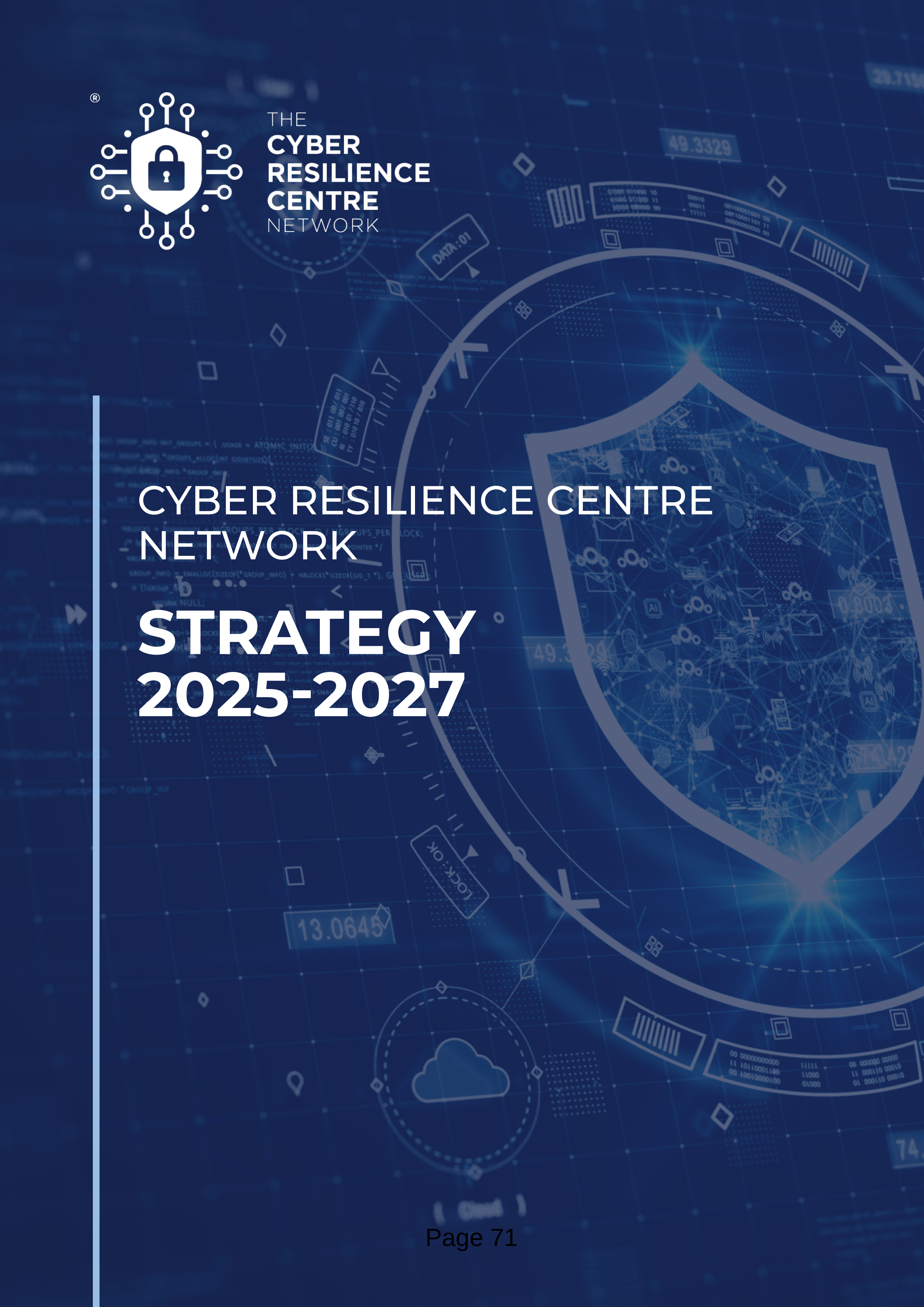
Appendices

- Appendix 1 – CRC Network Strategy 2025-27

Andrew Gould
Detective Chief Superintendent NPCC National Cybercrime Team

T: 07596 888450
E: andrew.gould@cityoflondon.gov.uk

This page is intentionally left blank



THE
CYBER
RESILIENCE
CENTRE
NETWORK

CYBER RESILIENCE CENTRE NETWORK

STRATEGY 2025-2027

TABLE OF CONTENTS

* This Strategy should be read in conjunction with the CRC Network Operating Model.

CRC NETWORK MISSION

The Cyber Resilience Centre Network is a strategic collaboration between the police, government, private sector and academia to help strengthen cyber resilience across the sole trader, micro, small and medium-sized enterprises and third sector communities, protect the UK economy and support growth. The CRC Network is a key part of HM Government's National Cyber Strategy and the National Policing Strategy for Fraud, Economic and Cyber Crime.

Small and medium-sized organisations (SMOs) accounted for 99% of the UK business population at the start of 2024, with 99% being small businesses with fewer than 50 employees[1] . Federation of Small Businesses research suggests that 77% of smaller businesses within the UK are part of supply chains[2] . Smaller organisations typically lack in-house expertise and may never have benefited from cyber resilience advice, due to a lack of awareness of cyber threats, cost, or not knowing where to start and who to ask for help.

The CRC Network proactively identifies ways to reach Small and Medium Sized Organisations (SMOs) to provide cyber security guidance, raising awareness and encouraging behaviour change to drive cyber resilience. The CRC Network promotes and aligns with services, products and guidance from the National Cyber Security Centre (NCSC). The network is "Police-Led, Business-Focused", capitalising on the police brand as a trusted source of crime prevention guidance and support.

The CRC Network provides long-term support, through a customer journey model, involving regular, engaging bitesize cyber security guidance to members, tailored to specific regions or sectors. The journey aims to develop understanding over time.

Cyber PATH provides SMOs with fully funded cyber security services such as staff training, guidance on security policy and testing services to improve their risk awareness and cyber resilience. The CRC Network works with some of the country's top student talent, with the students delivering these services. The CRCs encourage the onward referral of members to Cyber Essentials (CE) partners and CE certification. Cyber PATH is a unique programme for workplace ready talent, aiming to address the skills crisis in industry and public sector.

The **National Ambassador Programme** provides the UK's largest organisations with an opportunity to work in collaboration with policing, to promote cyber resilience to their SMO supply chains, client base and wider SMO community.

[1] *UK Small Business Statistics, Federation of Small Businesses*

[2] *Chain Reaction: Improving the supply chain experience for smaller businesses, Federation of Small Businesses Report 2018*

THE CRC NETWORK SUPPORTS HM GOVERNMENT'S NATIONAL CYBER STRATEGY 2022

1 PILLAR ONE:

STRENGTHENING THE UK CYBER ECOSYSTEM:

Strengthen the structures, partnerships and networks necessary to support a whole-of-society approach to cyber

Enhance and expand the nation's cyber skills at every level, including through a world class and diverse cyber security profession that inspires and equips future talent

Foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider economy

The CRC Network recognises that it cannot operate alone. Regional CRCs are a key part of their local Cyber ecosystem, engaging with the UK Cyber Clusters, local Chambers of Commerce, business and innovation groups and community volunteers to promote SMO cyber resilience.

2 PILLAR TWO:

CYBER RESILIENCE:

Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

Prevent and resist cyber-attacks more effectively by improving management of cyber risk within UK organisations, and providing greater protection to citizens

Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks

The overarching goal of the CRC Network, from which all activity flows, is for SMOs to **understand** cyber threats and **change their behaviour** to improve cyber resilience, making the UK a safer place.

CRC NETWORK VISION

The vision for the CRC Network is:

- ✓ To be the trusted source of cyber resilience guidance for SMOs, thereby making the UK a safer place to do business online
- ✓ To help members understand their cyber risks and improve their cyber security
- ✓ To help reduce the UK cyber skills shortage through Cyber PATH student development

CRC NETWORK STRATEGIC OBJECTIVES FY 25/26 – FY 26/27

1. Increase membership of priority sector - Managed Service Providers for SMOs
2. Increase membership of priority sector - SMOs holding large personal data sets
3. Supporting existing CRC members
4. Close alignment with National, Regional and Local Cyber Protect Teams
5. Integration with Cross-Government SMO cyber resilience projects and initiatives
6. Growing membership at scale, including through National Ambassador/large organisation campaigns across SMO customers and supply chains
7. Promotion of Cyber Essentials/Cyber Essentials+
8. Iterative improvement and innovation

ACHIEVING OUR CRC NETWORK STRATEGIC OBJECTIVES - RATIONALE AND PRINCIPLES

PRIORITY SECTORS - MANAGED SERVICES PROVIDERS FOR SMOS AND SMOS HOLDING LARGE DATA SETS.

While citizens and the wider economy are a clear priority for government in improving resilience, the Home Office, NCSC and DSIT have identified two key areas where significant widespread harm needs to be tackled.

The first is tackling the threat from infiltration of supply chains, particularly where there are digital connections allowing companies direct access into the systems of other organisations.

The second is tackling the stolen data ecosystem; protecting individuals from the downstream cybercrime and fraud attacks enabled by the exfiltration of data from cyber breaches against organisations. This is a particular concern where organisations hold data on vulnerable citizens.

SUPPORTING EXISTING CRC MEMBERS

We will improve our understanding of the impact that CRC membership and Cyber PATH services has on SMO awareness and behaviour; focusing KPIs and metrics on how engaged our membership is and what actions they took.

CLOSER ALIGNMENT WITH NATIONAL, REGIONAL AND LOCAL CYBER PROTECT TEAMS

As a key part of the wider law enforcement Team Cyber UK network, CRC Network activity will align with the National Policing Strategy for Fraud, Economic and Cyber Crime 2023 – 2028. Close working relationships with every part of the system; including Report Fraud, regional and force cybercrime teams, PCA and NCCU are vital to deliver as a collective; improving cyber resilience and reducing repeat victimisation.

INTEGRATION WITH CROSS-GOVERNMENT SMO CYBER RESILIENCE PROJECTS AND INITIATIVES

The CRC Network is increasingly seen as a delivery mechanism for HM Government departments to reach SMOs in every part of England and Wales, at a very local level.

As a key threat area, there are numerous different Government departments and agencies who have some involvement in cybercrime and cyber security. This poses a risk of duplication. The outcomes can include an inefficient use of limited resources, unmet demand and confused messaging to SMOs.

CRC Network activity must be situated within the wider context of cross-government objectives, with an aligned communication strategy.

GROWING MEMBERSHIP AT SCALE, INCLUDING THROUGH NATIONAL AMBASSADOR/LARGE ORGANISATION CAMPAIGNS ACROSS SMO CUSTOMERS AND SUPPLY CHAINS

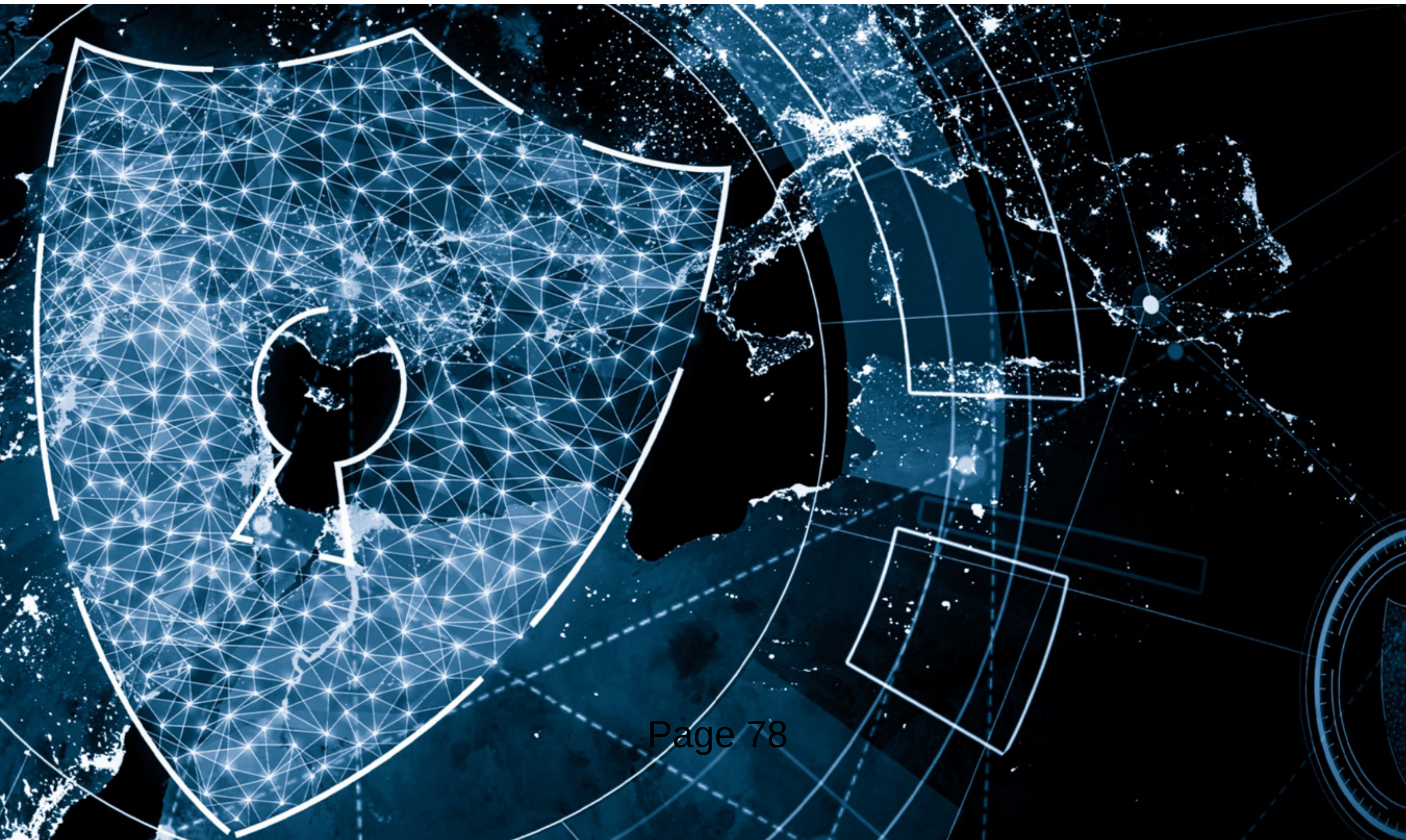
The CRC Network has limited staff and resources, and a potential target audience of over 5 million SMOs. The challenge is significant. The network must adopt a delivery model that is as efficient as possible; narrowing the target audience to focus on those most at risk, or where the impact of a cyber-attack would be most significant, and amplifying the message through strategic relationships and tailored marketing activity, rather than one-to-one engagement.

PROMOTION OF CYBER ESSENTIALS/CYBER ESSENTIALS+

Cyber Essentials represents the HM Government's minimum baseline standard for cyber security for organisations of all sizes in the UK. The annually renewable certification scheme is aligned to five technical controls designed to prevent the most common internet-based cyber security threats. Cyber Essentials certification demonstrates that an organisation is protecting itself by implementing the most important cyber security controls. Therefore, a key metric for the impact of CRC guidance and support, and demonstration of behavioural change, is for CRC members to go on to become Cyber Essentials certified.

ITERATIVE IMPROVEMENT AND INNOVATION

The network will be agile and innovative, able to test out new ideas and approaches to achieve the strategic objectives. Initiatives will be tested across multiple centres to draw on an evidence base as to what works and why. The network will proactively seek different ideas and perspectives from all staff, volunteers and local and national partners in industry and academia.



THE
CYBER
RESILIENCE
CENTRE
NETWORK

This page is intentionally left blank

Committee(s): Economic & Cyber Crime Committee	**Dated:** 23/2/26
Subject: Innovation & Growth – Update of Cyber & Economic Crime related activities	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties** • **provides business enabling functions**	Dynamic Economic Growth
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: Executive Director, Innovation and Growth	Damian Nussbaum
Report author: Head of FPS Technology, Innovation & Growth	Melissa Panszi

Summary

The core objective of Innovation & Growth (IG) is to strengthen the UK's competitiveness as the world's leading global hub for financial and professional services (FPS). This includes promoting the strengths of the UK's offer and enhancing the UK's position as a leader in FPS technology and innovation.

As the national lead force for fraud and NPCC lead for cyber, the City of London Police (CoLP) plays an important role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. The work of Innovation & Growth (IG) and CoLP therefore remains closely aligned.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime since the ECCC last convened in November 2025.

Links to the Corporate Plan

1. The activities set out in this report help deliver against the Corporate Plan's aim to support a thriving economy. This includes outcome 6c - to lead nationally and advise internationally on the fight against economic and cybercrime. It also supports outcome 7, positioning the UK as a global hub for innovation in financial and professional services.

Main Report

Innovation & Growth/City of London Police cross-team working

2. We continue to use this report to review those activities which demonstrate the benefits of IG and CoLP collaboration. IG continues to look for ways to promote the activity of CoLP and support their work as part of our wider stakeholder engagement.

Collaboration

3. As a result of the collaboration between the PAB and IG to engage with HMT on the forthcoming Financial Action Task Force (FATF) evaluation of the UK's anti-money laundering regime, the City is hosting FATF's Learning and Development Forum, a meeting of supervisors that supports the implementation of FATF's risk-based approach to standards. The forum will take place on 25–26 February at the Barbican, and a reception (sponsored by the Police Authority will be hosted at Mansion House.

Innovation & Growth activity

Economic Security – Business and Trade Committee of the House of Commons

4. On 24 November, the Business and Trade Committee of the House of Commons launched its report, "Toward a New Doctrine for Economic Security." The report sets out a framework for how the UK should develop a new economic security doctrine by identifying key threats, guiding principles, and required governance changes; benchmarking the UK against other jurisdictions; and providing actionable recommendations. The Corporation will be reaching out to Liam Byrne, Chair of the Business and Trade Committee, to discuss the City of London Corporation's interest in this space and explore potential areas for collaboration.

RegTech

5. Regulatory Technology (RegTech) focuses on developing technological solutions that enable regulated firms to meet compliance and regulatory requirements more efficiently and effectively. Last year the City of London Corporation (CoLC) and Innovate Finance launched the RegTech Strategy Group to position RegTech as a major UK export sector, contribute to the Government's wider growth agenda, expand the UK RegTech sector by 20%, and significantly reduce compliance costs over the next five years.

6. The RegTech Strategy Group held its first meeting on 15 October, where members discussed key priorities and challenges. This resulted in the development of a problem statement document presented at the second meeting on 15 January. At the second meeting, members endorsed the problem statements and volunteered to lead working groups across four priority areas identified: (1) data access to enable AI solutions, (2) technology-positive regulation, (3) digital identity infrastructure, and (4) investment and talent development.

Digital Verification

7. The City of London Corporation's Securing growth: the digital verification opportunity report (March 2025) articulated the need for UK-wide digital verification

service (DVS) to combat fraud of and introduce efficiencies into our financial system around the sharing of personal and organisational data. Such a system needs an underlining operating platform on which personal data, organisational data and other information can be shared safely and speedily. The Corporation's work is about setting up this operating platform - which we have been calling a Digital Verification Orchestrator (DVO). It is an industry-endorsed, governance-backed infrastructure, focused on fraud reduction, Smart Data enablement, and aims to fuel economic growth. To achieve this, the City of London is establishing a Digital Verification Orchestrator Strategy Steering Committee (SteerCo) and working group, which will:

- Expand participation in the orchestrator model
- Strengthen the link between industry and government on DV
- Feed into FCA efforts to standardise orchestration rules across the market

8. The programme will launch on 30 January 2026 and run through to June/July 2026. The SteerCo will be chaired, in an independent capacity, by Ezechi Britton MBE, with Sushil Saluja CC, Innovation and Tech Lead at the City of London Corporation, as Vice-Chair. Hogan Lovells will provide the secretariat and legal advice. Membership will include some of the UK's largest banks and FinTechs, alongside a working group comprising SteerCo firms, academics, trade associations and institutes, and advisers. HMT, FCA, DBT will observe and DSIT have committed to speaking at at least one meeting. This work supports the City Corporation's Vision for Economic Growth recommendation to scale digital verification across UK financial services.

Corporate & Strategic Implications

9. Strategic implications - This work supports the Corporate Plan outcome to drive dynamic economic growth.

10. Financial implications - All budgets are contained within existing departmental budgets and business planning.

11. Resource implications - All resourcing requirements are scoped as part of departmental business planning.

12. Legal implications - None identified for this paper.

13. Risk implications - None identified for this paper.

14. Equalities implications - The stakeholder work as part of this work is mindful of balancing the needs to have the right stakeholders identified while also supporting the CoLC's EDI commitments.

15. Climate implications - None identified for this paper.

16. Security implications - None identified for this paper.

Conclusion

IG will continue to engage with the CoLP and the PA on economic crime and cyber through the ongoing initiatives set out in this paper, as well as any emerging issues that may arise. We will also continue to engage with the CoLP in relation to its National Lead Force role.

Melissa Panszi
Head of FPS Technology
E: Melissa.Panszi@cityoflondon.gov.uk

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

Agenda Item 14

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.

Agenda Item 15

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

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

Agenda Item 17

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

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

Agenda Item 19

Document is Restricted

This page is intentionally left blank

Agenda Item 20

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