Public Document Pack

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

Date: **TUESDAY, 4 FEBRUARY 2025**

Time: 11.00 am

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

Members:

Deputy James Thomson CBE (Chair)
Tijs Broeke (Deputy Chair)
Nicholas Bensted-Smith
Alderman Professor Emma Edhem
Jason Groves
Deputy Madush Gupta
Sir Craig Mackey
Graham Packham
Deputy Dawn Wright
Mandeep Thandi,
Naresh Hari Sonpar,
Michael Landau (External Member)
Deputy Christopher Hayward,
James Tumbridge,

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

3. **MINUTES**

To approve the public minutes and non-public summary of the meeting held on 19 November 2024.

For Decision
(Pages 5 - 8)

4. **NATIONAL LEAD FORCE PERFORMANCE REPORT Q3 OCTOBER - DECEMBER 2024**

Report of the Commissioner.

For Information
(Pages 9 - 34)

5. **CYBER GRIFFIN UPDATE**

Report of the Commissioner.

For Information
(Pages 35 - 40)

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

Report of the Executive Director, Innovation and Growth.

For Information
(Pages 41 - 46)

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

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

9. **EXCLUSION OF THE PUBLIC**

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

For Decision

Part 2 - Non-Public Agenda

10. **NON-PUBLIC MINUTES**

To agree the non-public minutes of the meeting held on 19 November 2024.

For Decision
(Pages 47 - 48)

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

Report of the Commissioner.

For Information
(Pages 49 - 74)

12. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE - REGULAR PROGRAMME PROGRESS NOTE**

Report of the Commissioner.

For Information
(Pages 75 - 168)

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

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

This page is intentionally left blank

ECONOMIC AND CYBER CRIME COMMITTEE OF THE CITY OF LONDON POLICE AUTHORITY BOARD
Tuesday, 19 November 2024

Minutes of the meeting of the Economic and Cyber Crime Committee of the City of London Police Authority Board held at Committee Rooms, Guildhall on Tuesday, 19 November 2024 at 9.30 am

Present

Members:
Deputy James Thomson (Chair)
Jason Groves
Deputy Madush Gupta
Graham Packham

Officers:

Richard Riley CBE	-	Town Clerk's Department
Oliver Bolton	-	Town Clerk's Department
Kezia Barrass	-	Town Clerk's Department

City of London Police

Chris Bell	-	City of London Police
Eleanor Summers	-	City of London Police

1. **APOLOGIES**
Apologies were received from Tijs Broeke, Naresh Sonpar, Nick Bensted-Smith, Michael Landau, Sir Craig Mackey and Dawn Wright.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
There were no declarations.

3. **MINUTES**
RESOLVED, - that the public minutes and non-public summary of the meeting held on 16 September 2024 were approved as an accurate record.

4. **NATIONAL LEAD FORCE PERFORMANCE PACK**
Members received a report of the Commissioner which provided an outline of the National Lead Force performance.
Members felt that the report would benefit from the inclusion of an executive summary to provide a full picture and narrative of what the data is showing. Members felt that the executive summary should reflect a strategic overview of performance with summarised highlights.
Members suggested a workshop be organised with key officers and Members to provide further feedback on the report.
RESOLVED, - that the report be noted.

5. **CYBER GRIFFIN UPDATE**

Members received a report of the Commissioner which provided an update on Cyber Griffin work.

Members noted recent positive discussions which had taken place with the Home Office around the Spending Review. The Chair emphasised the need to continue with the momentum developed. Members felt that services in the report should have clarified definitions and should evidence the outcomes more than the activities.

RESOLVED, - that the report be noted.

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

Members received a report of the Executive Director Innovation and Growth which provided an update of cyber and economic crime related activities.

Members noted the ongoing work with marketing colleagues to develop a robust communications strategy which would involve proactive engagement.

The Chair noted the absence of reporting on economic security and requested that any future reports include an update on the development of economic security in the City of London.

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**

There was no other business.

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 items of business on the grounds 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 16 September 2024 were approved as an accurate record.

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

Members received a joint report of the Commissioner and the Town Clerk which outlined the strategic communications and engagement plan for economic and cyber crime.

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

There were no questions.

13. **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 10:33

Chairman

Contact Officer: Kezia Barrass
Kezia.Barrass@**cityoflondon.gov.uk**

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Economic and Cyber Crime Committee – for information	**Dated:** 4 February 2025
Subject: National Lead Force Performance Pack	**Public**
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 Police
Report author:	Lucy Cumming

Summary

This report is the most recent National Lead Force (NLF) Performance Pack that is produced quarterly and presented to the ECCC.

The performance pack reflects the objectives and measures set within the National Policing Strategy for Fraud, Economic and Cyber Crime and includes national performance in the areas that City of London Police, under NLF functions, lead and co-ordinate.

Recommendation(s)

Members are asked to:

- Note the report.

This page is intentionally left blank

National Lead Force
City of London Police Performance Report

Q3: October – December 2024

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:	Q2	Q3
We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.	⇧	⇧
We will deliver enhanced victim care & support to victims of fraud & cyber crime, to reduce harm of offending and prevent re-victimisation.	⇧	⇧
We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.	⇧	⇧
We will improve the policing response to fraud. Fraud and Cyber Reporting and Analysis Service (FCCRAS) objectives will be added when the system launches.	⇧	⇨
We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages	⇧	⇨
We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.	⇩	⇧
We will upskill and train our staff so that they are able to effectively respond to the threat of fraud, economic and cyber crime.	⇧	⇨
We will develop and action a National Economic Crime Workforce Strategy.	⇨	⇧

Executive Summary: Key Cross Cutting Strategic Objectives

Protect disruptions and social media impressions have exceeded the Home Office target significantly. This is due in part to press release in August regarding retail fraud and a DCPCU interview on BBC Morning Live which promoted engagement with social media.

National Lead Force hosted and organised a number of key strategic events in Q3:-

National Strategic Economic Crime Briefing – 190 attendees from police forces, regional crime units, NCA, NPCC, CPS and NECC.

SOCEX – 400 operational law enforcement professionals, government and industry representatives.

NUG (National User Group) –200 attendees. Forces from all over the country attended.

Protect Conference –200 officers and staff. The very first joint protect conference which brought together both the fraud and cyber protect networks.

National Lead Force has exceeded its Home Office set target for judicial outcomes by a significant percentage. This is due to a number of outcomes linked to two large investigations in Q1 and Q2.

NFIB have implemented use of the new Foundry Platform in Q3. This has led to temporary abstractions of st7-dayiod to training and facilitating the launch of the new system.

NFIB sent less vulnerable person alerts this quarter, however 99% were sent within the 7-day target. There has been a drop in NFIB performance this quarter due to staff abstractions.

Action Fraud satisfaction has fallen 4% below the Home Office target.

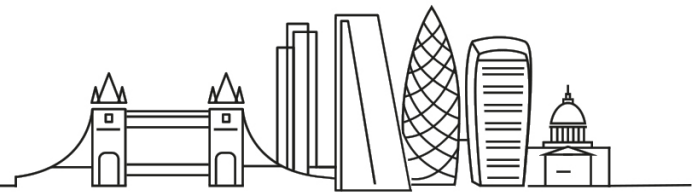
NECVCU performance has been affected by staff abstractions due to training leading to a lower volume of calls being made.

Disruptions against organised crime groups are increasing. In Q3, NLF Ops teams recorded major disruptions for investigations into payment diversion and investment fraud.

Financial disruptions are also increasing. Following a successful investigation into a £2.7 million boiler room fraud, CoLP successfully applied for confiscation orders, with 134 victims being paid from the available £372,742.

National Lead Force operational teams supported the national money mule intensification Operation Emma 10.

CITY OF LONDON POLICE

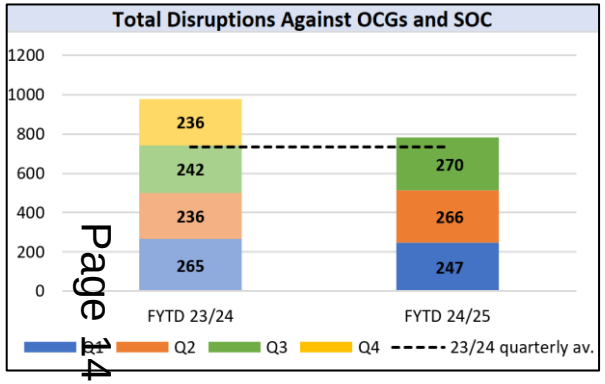


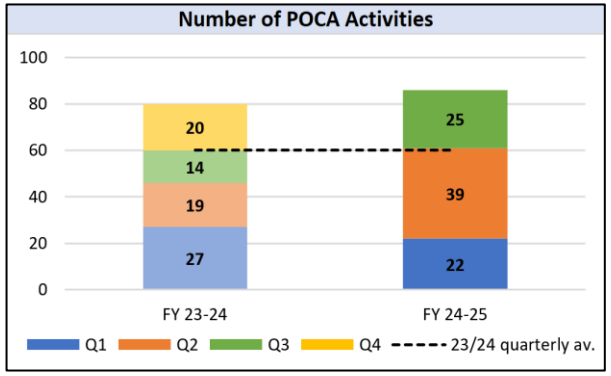
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

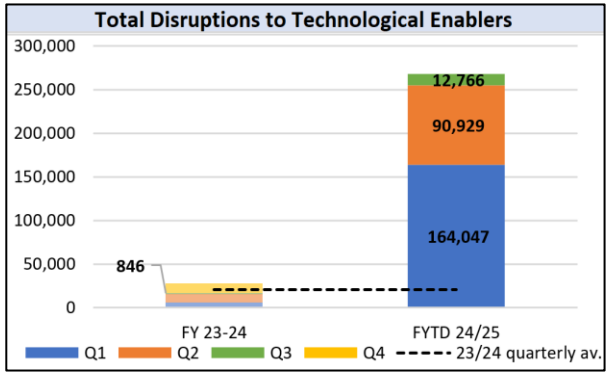
Proactively Pursue Offenders

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 and serious organised crime	⇧
B. Increase the number of POCA activities	⇧
C. Increase the number of disruptions against technological enablers	⇧







OCG Disruptions

- Teams are investigating **65** OCGS (-5)
- In Q3 teams recorded against OCGs:
- **4 major** disruptions (= to 23/24 Q3)
- **4** moderate (-5 on 23/24 Q3)
- **11** minor disruptions (+3 on 23/24 Q3)
- **248** disruptions against other threats is a **+12% (+27)** increase on Q3 23/24

Financial Disruptions

- In Q3 Fraud Teams reported **29** POCA activities up **79% (+11)** from Q3 23/24
- These had a value of **£1,913,501** down **4% (-£86,644)** from Q3 23/24
- **7** confiscations, **3** asset restraining, **12** cash detentions and **3** cash forfeitures
- **170** victims were awarded a share of **£797,896** in compensation

Technological Disruptions

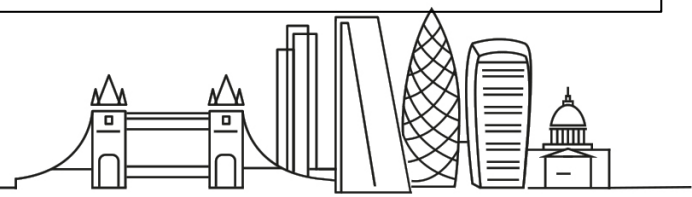
In Q3 Fraud teams reported:

- **239** disruptions to websites
- **12,522** to cards and bank accounts
- **5** to social media accounts
- **1,410% (+11,920)** increase on Q3 23/24
- **DCPCU** carried out large operations resulting in more than 265k bank account shut-downs in March, July and November

Disruptions

In Q3, **NLF Ops** teams recorded major disruptions for investigations into payment diversion and investment fraud. A female carer was convicted of Abuse of Position of Trust and sentenced to 30 months suspended for 3 years, and a corporate employee fraud defendant received 3 years imprisonment. **PIPCU** worked with law enforcement across Europe to take down a large illegal streaming network. **DCPCU** saw 3 men sentenced to a combined 6 years 9 months for using a SIM farm to defraud victims of over £223k and **IFED** recorded 3 convictions for staged motor collisions.

Following a successful investigation into a £2.7 mil boiler room fraud, **CoLP** successfully applied for confiscation orders, with 134 victims being paid from the available £372,742.



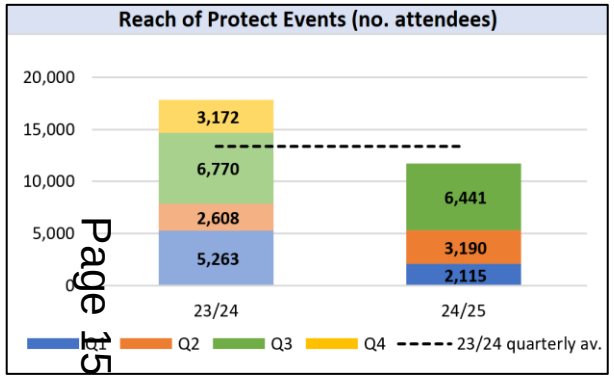
CITY OF LONDON POLICE

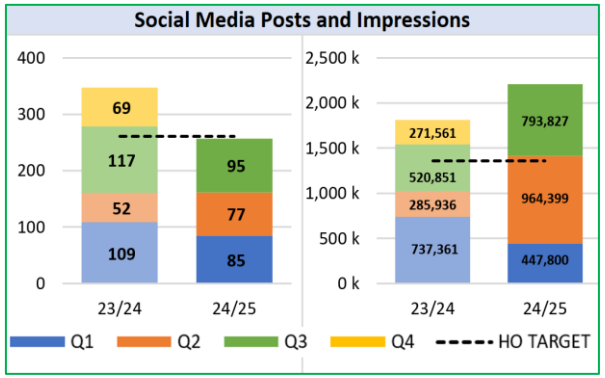
National Lead Force Fraud Operations: Includes National Fraud Squad Teams and Funded Units

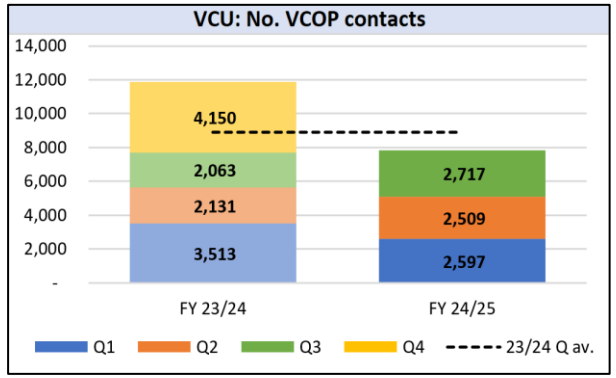
Protect People and Businesses

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 – **Home Office Measure**	⇧
C. Increase the number of Victim Support Unit contacts	⇧







Protect Events

- Teams held **65** events in Q3 a **35% decrease (-34)** from Q3 23/24
- **6,441** people attended these events down **5% (-329)** from Q3 23/24
- Activity peaked in November with **33** events and **3,626** attendees

Social Media – HO Measure

- Teams posted **95** messages on social media, down **18% (-22)** from Q3 23/24.
- The related impressions rose to **793,827**, up **52% (+272,976)** on Q3 23/24
- Impressions were particularly high in August due to a press release regarding a retail fraud investigation
- **Home Office target Exceeded**

Victim Care Unit

- VCU was responsible for **4,683** victims in Q3, relating to **25** (+3) investigations.
- A total of **2,717** VCOP updates were issued in Q3, up 32% (+654) from Q3 23/24
- **1,436** victims received Protect advice
- **4** new call blockers were issued, and **159** nuisance calls were blocked in Q3

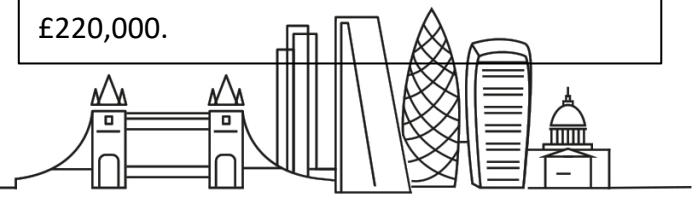
PROTECT and Social Media

IFED posted regarding moped 'crash for cash' fraud. Other media included a quote by the A/Commissioner on the new Insurance Fraud Charter and an interview in The Economist.

The **NLF Ops** teams posted about romance fraud, featuring protect advice from celebrities, and publicised International Fraud Awareness Week.

The **PIPCU** DCI was interviewed by the BBC about the risks of fake car parts and ITV about fake goods before Christmas.

DCPCU's interview on BBC Morning Live was engaged with on social media. A press release was sent on 3 men sentenced for sending phishing messages and stealing over £220,000.



CITY OF LONDON POLICE

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

Improve Outcomes for Victims

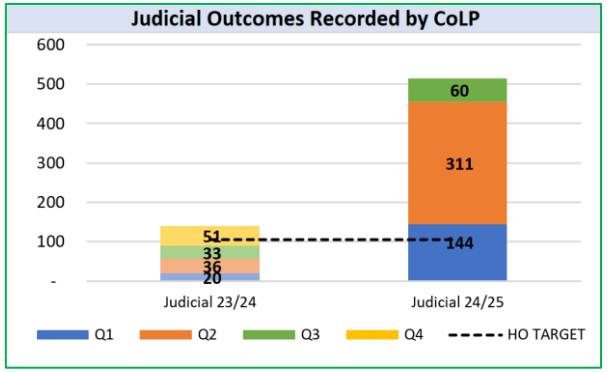
We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout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

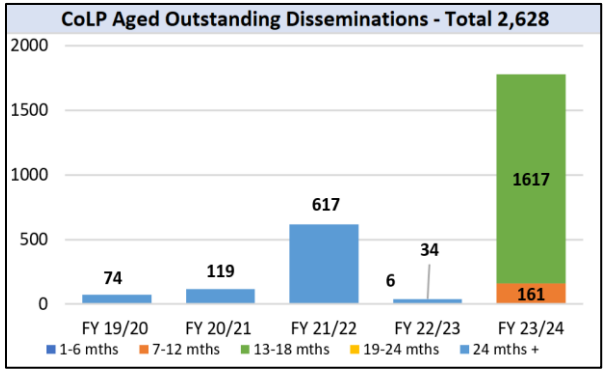
Success Measures:	
A. Increase the judicial outcome rate for CoLP – **Home Office Measure**	⇧
B. Decrease CoLP aged outstanding disseminations	⇧
C. Support CoLP teams to engage in intensification efforts – **Home Office Measure**	⇧

LFOR intensifications – HO Measure

The CoLP Fraud Targeting Cell (FTC) disseminated 14 intelligence packages to the Proactive Economic Crime Teams (PECTS) as part of the EMMA 10 intensification. The FTC worked closely with the Cyber Defence Alliance to identify Money Mule Recruiters advertising services on social media.

Throughout November 2024 7 suspects were arrested relating to the packages. The interview of another suspect resulted in a Cease and Desist notice. There was positive feedback from the PECTs who commented on the proactive nature of the operation and comprehensive detail of the intelligence packages. **Home Office target met**





Judicial Outcomes – HO Measure

- In Q3 CoLP teams recorded **60** judicial outcomes
- Up **81% (+27)** from Q3 23/24, but down 81% from the previous quarter.
- **222** no further action outcomes were also recorded, up **95% (+108)** from Q3 23/24
- **Home Office target Exceeded**

Outstanding Disseminations

- At the end of Q3 **2,628** disseminations from 19/20 to 23/24 were with CoLP teams awaiting outcomes.
- This is down **-5.54% (-154)** from the end of the previous quarter showing ongoing improvement

Judicial Outcomes

A national target of 6,000 judicial outcomes was set for 24/25, and this has now been exceeded by 5% with 6,275 outcomes reported. The combination of a number of large cases being finalised and the continued targeted engagement from the National Coordinators Office have been instrumental in reducing outstanding disseminations.

CoLP teams have contributed to this result with judicial outcome totals consistently above the 23/24 average.

61% of the 24/25 judicial outcomes recorded by CoLP are from two large NLF investigations recording 105 outcomes in Q1 and 209 in Q2.

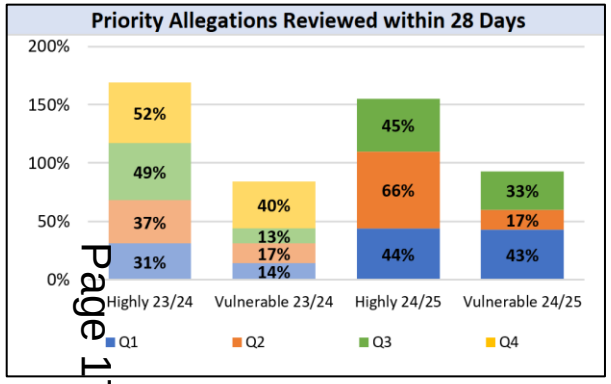
National Reporting Service: Includes NFIB, Action Fraud (AF) and NECVCU

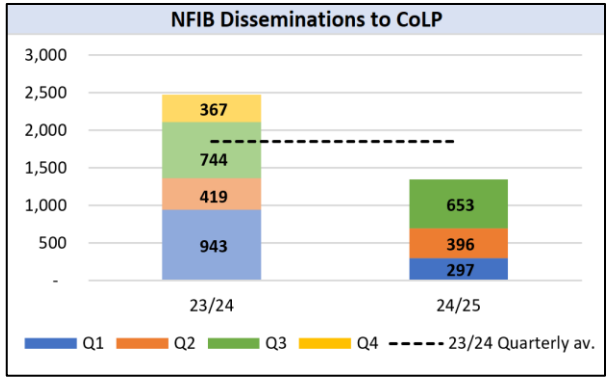
Proactively Pursue Offenders

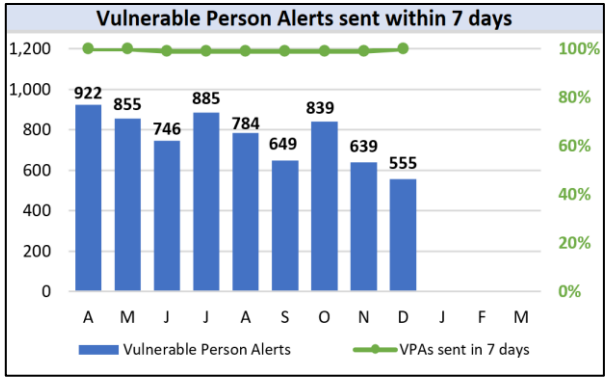
We will deliver the Fraud and Cyber Reporting and Analysis Service (FCCRAS) - including the ability to feedback intelligence into the system for further development and inclusion in intelligence packages. We will ensure intelligence is appropriately recorded and disseminated to assist with all 4P outcomes

Success Measures:

A.	Increase the allegations of fraud reviewed in 28 days meeting 'highly likely' & 'likely vulnerable' on the solvability matrix	⇧
B.	Increase the number of NFIB packages disseminated to CoLP teams	⇩
C.	To review and, where appropriate, disseminate vulnerable person alert within 7 days.	⇨







Priority Allegations

- In Q3 NFIB teams reviewed:
- **45%** of allegations that are highly likely to be solved, down **4%** from Q3 23/24
- **33%** of 'likely to be solved' with a vulnerability element, up from 13% Q3 23/24 and 17% the previous quarter

Disseminations to CoLP

- NFIB sent **653** disseminations to CoLP teams in Q3
- This was down **12% (-91)** on Q3 23/24 but up **65% (+257)** on the previous quarter
- In the same period all NFIB disseminations fell by **36% (-9,475)** from Q3 23/24 from 26,529 to 17,054

Vulnerable Person Alerts

- NFIB sent **2,033** vulnerable person alerts to forces in Q3
- This is a decrease of **12% (-285)** alerts from Q3 23/24
- Consistently, **99%** of these were sent within the 7-day target timescale

National Fraud Intelligence Bureau (NFIB)

In Q3 the NFIB undertook implementation of a new platform alongside their existing technology. Although it was intended to have no parallel running, there is now an incremental change from the current service to the new platform whilst the build for the front-end service goes live.

This has seen the abstraction of staff to facilitate the process and 22 coaches trained to use the platform and given opportunities to familiarise themselves with the new system, before cascading the training to staff when it goes live.

In Q1 and Q2 NFIB supported MPS investigation Stargrew, disseminating 20k allegations and affecting business as usual.

CITY OF LONDON POLICE

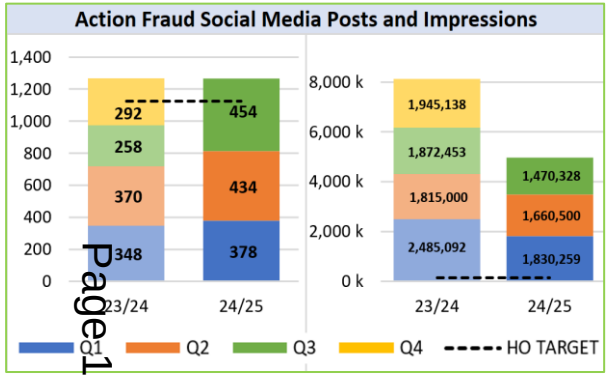
National Reporting Service: Includes NFIB, Action Fraud (AF) and NECVCU

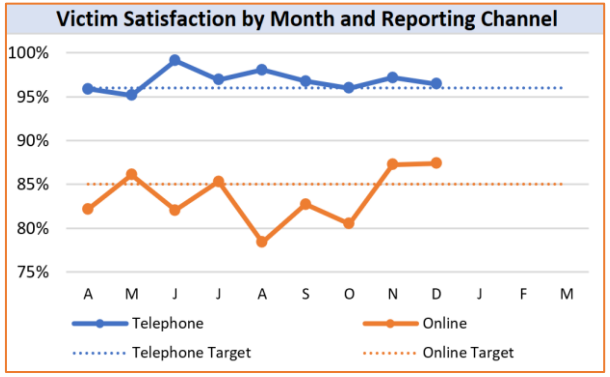
Improve Outcomes for Victims

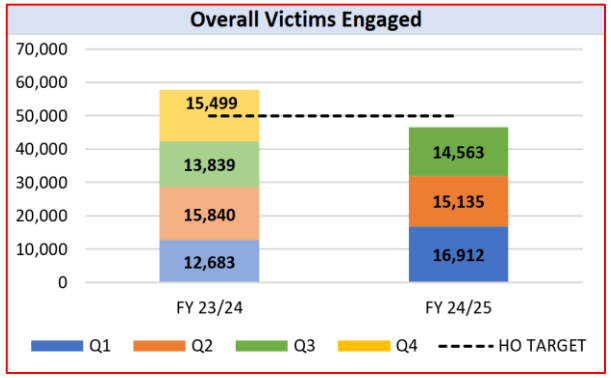
We will improve the policing response to fraud.
Fraud and Cyber Reporting and Analysis Service (FCCRAS) objectives will be added when the system launches.

Success Measures:

A.	Increase the number of Action Fraud social media posts and impressions – **Home Office Measure**	⇨
B.	Maintain the percentage of survey respondents who are satisfied with the Action Fraud reporting service – **Home Office Measure**	⇨
C.	Increase number of fraud victims who receive protect advice (NECVCU engagement) – **Home Office Measure**	⇩







Social Media – Action Fraud (AF) has increased collaboration with 3rd parties who post campaign materials, but the impressions are not logged in these figures. AF plan to implement videos and reels to expand reach and engagement from Q4.

Action Fraud - The Contact Centre focus remains consistent, maintaining FTE delivery across each shift, ensuring levels remain stable, and reducing average call waiting times, which fell from 11.53 minutes in Q2, to 9.28 in Q3.

NECVCU – Engagement is up compared to 23/24 but has not met the stretch target. Level 1 service levels were affected by staffing investment in training, workshops and support for continuous improvement measures between August and November, reducing the number of hours available for calls.

Action Fraud Social Media – HO Measure

- AF made **454** posts in Q3, up **75% (+196)** from Q3 23/24
- The related impressions for these posts totalled **1,470,328** a drop of 21% (-402,125) from the previous year
- **Home Office target Exceeded**

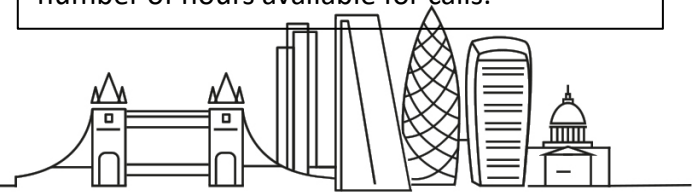
Action Fraud Satisfaction – HO Measure

- Contact Centre satisfaction was at **97%** in Q3, 2% higher than the 95% target
- Online reporting stable at **85%**, averaging out at the target rate
- Of the Overall, links delivered in Q3 just **1.1%** chose to provide satisfaction feedback
- Call abandonment was at 42%, up 15% from Q3 23/24
- **Overall, 4% below Home Office Target**

NECVCU Victim Contacts – HO Measure

- NECVCU engaged **14,563** victims, down **12% (-2,072)** from the HO target but up **5% (+724)** from Q3 23/24
- **£403,622** of funds were recovered, up **8% (+£28,622)** from the HO target
- **0.46%** repeat victims meets HO target
- **76%** victims feel confident online after engagement meets HO target
- **Home Office engagement target not met**

CITY OF LONDON POLICE



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 crime. We will roll out a revised performance framework across PURSUE, PROTECT, PREPARE and PREVENT. ROCUs and Forces to ensure completion of performance framework and resulting recommendations. We will invest in and explore technological and data sharing solutions and opportunities.

Success Measures:

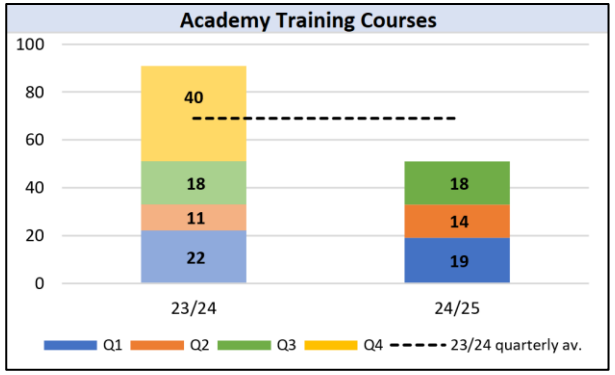
A. To increase delegate training levels in the Economic and Cyber Crime Academy (ECCA).	⇨
B. Deliver objectives against National Workforce Strategy.	⇧
C. National Coordinator's Office to complete visits to all ROCUs – **Home Office Measure**	⇨

Workforce Strategy

The FIO student placement program, has reached a significant milestone: students are embedded into CoLP with FIO accreditation. They are taking on meaningful and impactful responsibilities. Preparations for the second cohort are well underway.

The direct entry detective recruitment pathways for fraud and cybercrime are progressing positively. Fourteen recruits are set to begin their training in the PoliceNow academy/ CoLP this March.

Progress has been made in the development of the Living Library and the joint PwC/PSFA challenge panels, both of which are on track for launch by the end of February.



Academy

- In Q3 the ECCA held **18** courses, **equal** to the number in Q3 23/24
- The number of classroom delegates also stayed the same at **209** up 2 from 207
- Satisfaction at **88%** fell by **-2%** from Q3 23/24 due to poor venue in November
- Crypto training delegates continued to rise to **584** in Q3, compared to a total of 72 for the whole of 23/24.

ECPHQ Activity

National Strategic Economic Crime Briefing – 10 October, the Barbican, London, around 190 attendees from police forces, regional crime units, NCA, NPCC, CPS and NECC.

SOCEX – 18-20 November, Stratford-upon-Avon, over 400 operational law enforcement professionals, government and industry representatives.

NUG (National User Group) – 27 November, Birmingham, over 200 attendees. Forces from all over the country attended.

Protect Conference – 28-29 November, Birmingham, around 200 officers and staff who work in protect with representatives from every region. The protect conference was the very first joint protect conference which brought together both the fraud and cyber protect networks.

Regional Visits – Home Office Measure

In Q3 three regions were visited, NWROCU on 15/16 October, SWROCU on 12/13 November and the NWROCU on 9/10 December. All demonstrated some excellent working practices that can be shared across the regions.

One observation was inconsistencies in how disruptions are identified and recorded on APMIS, particularly in respect of Protect activity. There are also inconsistencies with the hosting of regional threat groups and strategic governance groups (prosperity). Lastly, the influx of new staff (AMLAR, Fraud Reform) has stretched supervisory ratios beyond the recognised norm for some regions.

Home Office measure ongoing

National Lead Force
National Delivery Plan Performance Report

Q3: October – December 2024

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		Q2	Q3
MLAR 1	We will increase criminal justice outcomes and disruptions against money laundering offenders.	⇩	⇧
MLAR 2	We will seize and restrain more criminal assets through including released asset denial activity	⇧	⇧
MLAR 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 NFIB / FCCRAS 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 NFS 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 NECC 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

		Q2	Q3
Fraud 6	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.	⇧	⇧
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 CyberAlarm 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 CyberAlarm to all SME organisations they engage with.	⇩	⇩
Cyber 5	We will deliver the new NPCC Cyber Resilience Centre (CRC) Model. This includes the new Operating Model to deliver the levels of consistency and assurance required. CRCs and PROTECT officers will work together to support each other's work and grow CRC membership.	⇧	⇧
Cyber 6	We will develop improved referral process for new nominals to include Target Operating Model and definition of when a referral should be made. We will introduce a single national or regional referral mechanism and implement risk assessment (CORA) and tasking mechanisms for PREVENT referrals.	⇧	⇧
Cyber 7	We will roll out the Cyber & Digital Specials & Volunteers (CDSV) Programme and platform to every region and Force and ensure effective management and utilisation of CDSV skills across the network.	⇩	⇧
Cyber 8	We will revise and roll out a clear training, CPD and accreditation pathway for all roles within TCUK, with regular reviews of the training needs analysis and advancements in technology / threats. NPCC Deliver new strategy and delivery with the Economic and Cybercrime Academy.	⇩	⇩

Executive Summary: Key Cross Cutting Strategic Objectives

NFIB disseminations out to law enforcement are exceeding the Home Office Target. This is in part due to the exceptionally high number of disseminations in Q1 under a large national target let operation (Stargrew), however Q3 is higher than the previous year's average.

There has been a 68% increase in judicial outcomes in comparison to the previous year. The Home Office quarterly target has been exceeded by 32%. This is due to high levels of outcomes attributed to national target led operations, and also the increase in resources investigating fraud in regional units.

National cyber judicial outcomes are showing a 41% decrease compared to the previous year. This is in part due to the high number of outcomes recorded in 23/24 Q2 which skewed the figures

Money laundering disruptions and asset seizures are increasing – exceeding the Home Office target. This is highly likely to be due to the increase in resource delivered to regional crime units under the AMLAR Programme which is co-ordinated by CoLP. So far 93 extra staff have been delivered nationally. Asset seizures were £11m this quarter - £6m of which was from one operation in the North West targeting a solicitor who was enabling money laundering. Overall cryptocurrency seizures are reporting an £15,839% (+£9,389,376) increase in comparison to 23/24. This is due to the use of new powers under the Economic Crime and Corporate Transparency Act, alongside upskilling and national procurement of analysis services by CoLP.

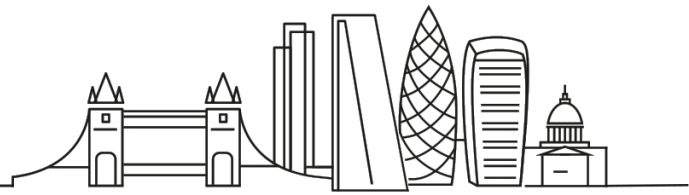
Operation EMMA 10 took place, targeting higher harm individuals responsible for recruiting money mules online (mule herders). The national operation resulted in 76 arrests, 43 warrants, £818,000 in seizures of cash and cryptocurrency, 13 asset freezing orders and 153 cease & desist notices and was a great success. City of London Police co-ordinated the policing response and provided actionable intelligence nationally.

National Protect surveys are now being issued at events nationally. The survey data for the first quarter has been useful in gaining quantitative and qualitative feedback from attendees at events hosted by the National Fraud Protect Network. 98% of attendees were satisfied with their engagement, with 96% likely to change their behaviour. Completion of these surveys is a target set by the Home Office

In Q3 National Protect disruptions have exceeded the Home Office target due to the high level of activity being undertaken by the new National Protect Network.

There has been an increase to the number of Cyber Crime Unit referrals to Cyber Resilience Centres.

CITY OF LONDON POLICE

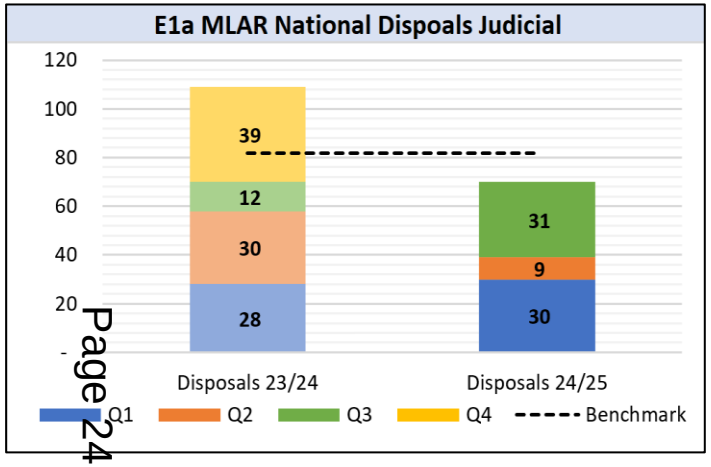


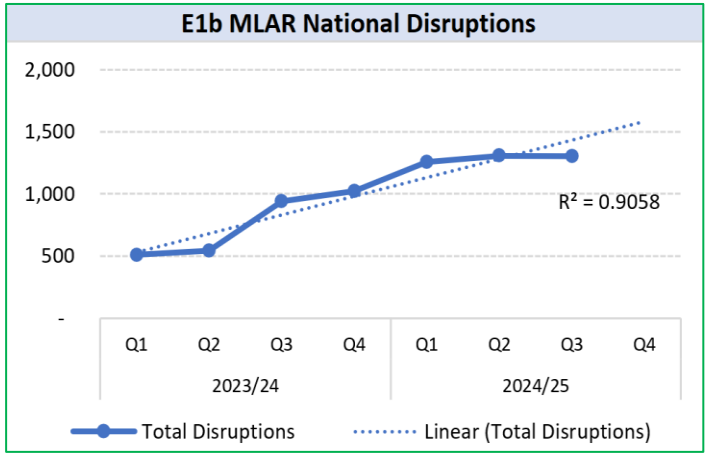
Money Laundering and Asset Recovery

Improve Outcomes for Victims

Performance Measure 1: We will increase criminal justice outcomes and disruptions against money laundering offenders.

Success Measures:	
E1a Increase judicial outcomes for money laundering cases.	⇩
E1b Increase the number of disruptions at all levels – **Home Office Measure**	⇧





E1a Currently, there are no judicial outcomes recorded for money laundering and asset recovery on APMIS, as they are not tracked under the current Home Office framework. However, we can measure judicial disposals within the Criminal Justice System. These are now counted towards the KPI measures of Judicial Outcomes. This data is likely under-reported.

For Q3, 31 judicial disposals were recorded, this is 158% (+19) increase compared to Q3 for the previous year.

2024/25 is reporting 70 judicial disposals so far, this is 14% (-12) under the benchmark target from 23/24.

E1b Money laundering and asset recovery is classed as illicit finance on APMIS. In Q3, there were a total of 1,302 disruptions.

- **66 major** - 5% increase (+3) in comparison to Q3 23/24
- **251** moderate - 70% increase (+103) in comparison to Q3 23/24
- **953** minor - 33% increase (+237) in comparison to Q3 23/24

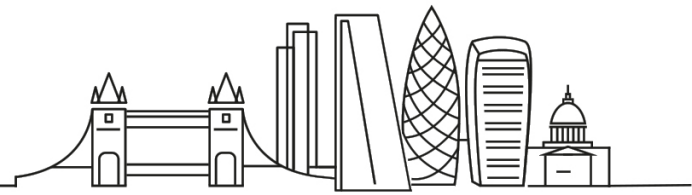
The benchmark from 23/24 was 3,019, which translates to 755 disruptions per quarter. For Q3, disruptions are 72% (+547) above the benchmark target. Overall, a positive quarter for disruptions.

Home Office Target Exceeded

The **Agency and Partner Management Information System** (APMIS) is the performance reporting and tasking system for the NCA and partners. The majority of data in this report is taken from this system.

APMIS was rolled out to all forces in 2023. The number of forces that are loading fraud, economic and cyber crime data is growing as forces obtain more licenses, however this is still a work in progress.

CoLP is encouraging all forces and regions in the use of APMIS during regular force engagement visits.

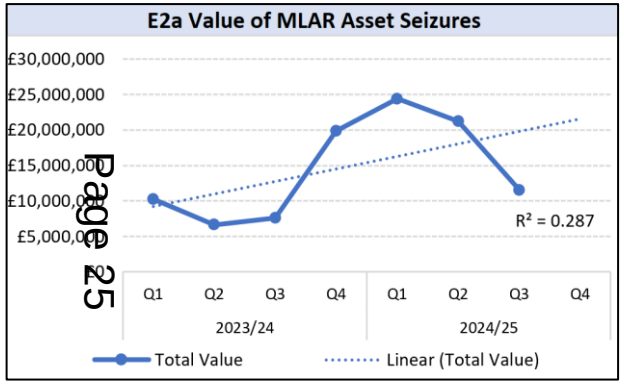


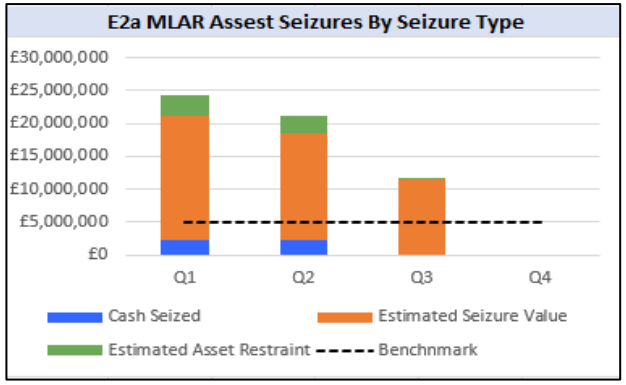
Money Laundering and Asset Recovery

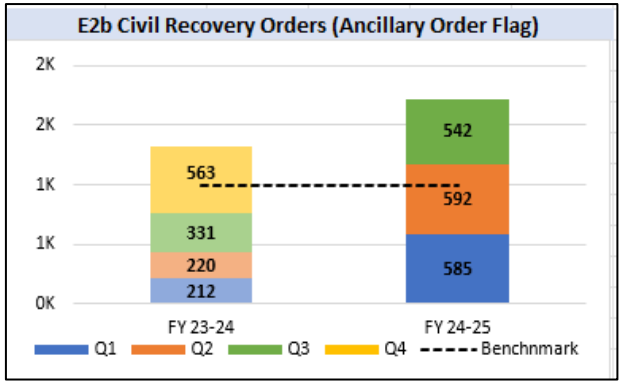
Proactively Pursue Offenders

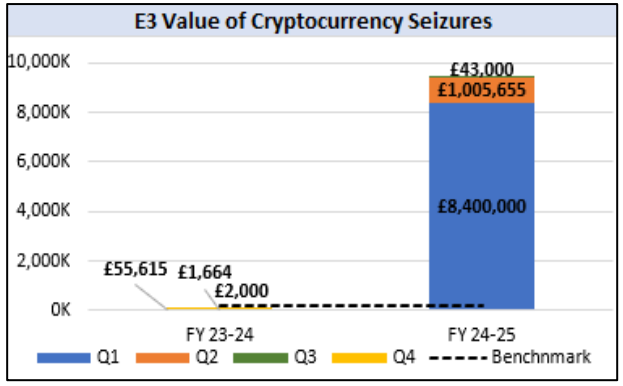
Performance Measure 2: We will seize and restrain more criminal assets through including released asset denial activity
Performance Measure 3: We will provide training to policing on how to investigate and seize crypto assets. We will ensure accurate records of crypto assets seizures are maintained and provided.

Success Measures:	
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.	⇧









E2a In Q3 a value of £11,662,880 asset seizures were recorded for money laundering and asset recovery. This is a 52% (+£3,952,434) increase from the same period in 23/24, and 137% (+£6,678,692) above the 23/24 quarterly average. The value has dropped in comparison to the previous quarter, but the annual figure is showing a significant rise. The North West seized £6M from one operation targeting solicitors facilitating money laundering.

E2b Previously, civil recorder orders were unavailable. Most civil recoveries are recorded as either disruptions in APMIS, or via a flag for Ancillary Orders. Please note that these figures are subject to change. Q3 is reporting a 63% increase (+211) in comparison to the same period in 23/24. Overall, figures are reporting at 30% (+393) above the benchmark for 23/24.

E3 For Q3, there has been £43,000 in cryptocurrency seizures. Q3 is reporting 23% (-£12,615) below the quarterly benchmark, however, overall cryptocurrency seizures are reporting an 15,839% (+£9,389,376) increase in comparison to 23/24. This increase can be explained by the new powers that came into force this year for crypto asset seizures.

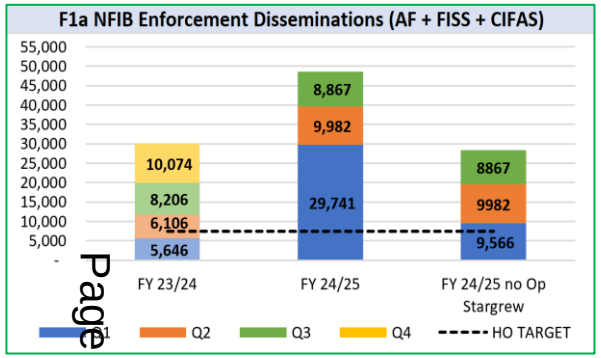
It is believed that all ROCUs are seizing crypto assets, and in the last year ROCUs have also corrected some input errors on APMIS, inflating the 24/25 figures in comparison to 23/24.

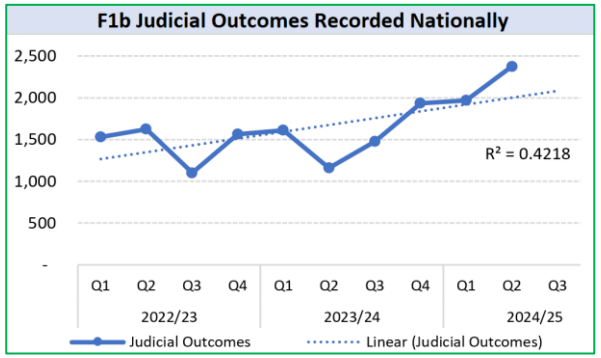
Fraud

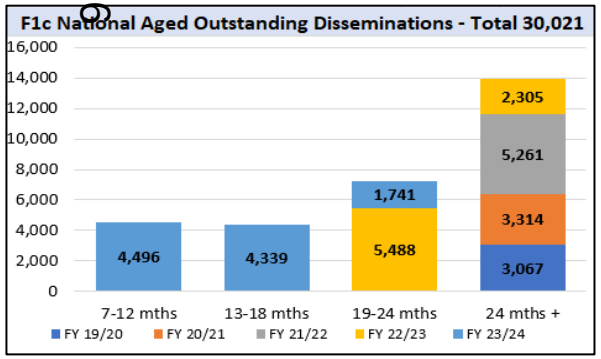
Improve Outcomes for Victims

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

Success Measures:	
F1a Increase the number of NFIB Pursue disseminations received and alternative positive outcomes (Outcome 22) – **Home Office Measure**	⇧
F1b Improve the judicial outcome rate and the alternative positive outcome rate – **Home Office Measure**	⇧
F1c Reduce the percentage of outstanding returns.	⇧







F1c For aged outstanding disseminations, data up to November 2024 reports 44% (49,466) of disseminations are marked as outstanding for England and Wales.

In comparison to Q2 24/25, this is a 6% decrease (-1,820), which is positive.

F1a NFIB disseminations increased in Q3 by 11% (+661) in comparison to Q3 for the previous year. Q1 reported a large increase due to Met led operation Op Stargrew, targeting a web-based platform described as a one-stop shop for phishing. Q2 & Q3 are reporting figures closer to normal range, however still considerably larger than the previous year's average. A reason for this is that the National Coordinator's Office have continued working with forces to reduce their aged disseminations, particularly across the periods of 2019-20 to 2021-22. Forces have responded positively to this work. **Home Office Target Exceeded**

We are currently not able to measure alternative positive outcomes due to changes being made within the Home Office counting rules.

F1b Nationally, there have been 2,373 judicial outcomes during this period and 10,985 non–judicial outcomes. This represents a 68% (+964) increase in judicial outcomes in comparison to the previous year. NFA outcomes have increased by 18% (-1,653) in the same period. The Home Office quarterly target of 1,547 has been exceeded by 32% (1,481).
Home Office Target Exceeded

All 45 forces were compliant in providing outcome information in a timely manner in Q3.

CITY OF LONDON POLICE

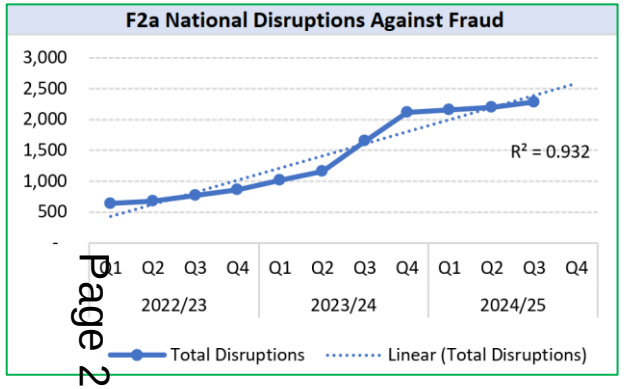
Total outcomes reported in a period can relate to disseminations from any time. The volume of outcomes fluctuates throughout the year as cases with varying numbers of crimes attached are completed. E.g. an investigation into a boiler room might have hundreds of outcomes attached to it and closing the case will give many outcomes, potentially bringing closure to multiple victims.

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:	
F2a Increase the number of disruptions against Fraud – **Home Office Measure**	⇧
F2b Increase the number of disruptions against Fraud organised crime groups (OCGs).	N/A



F2a Nationally there were 2,282 disruptions recorded for Q3. This is 39% above the quarterly benchmark for 23/24 (+635).

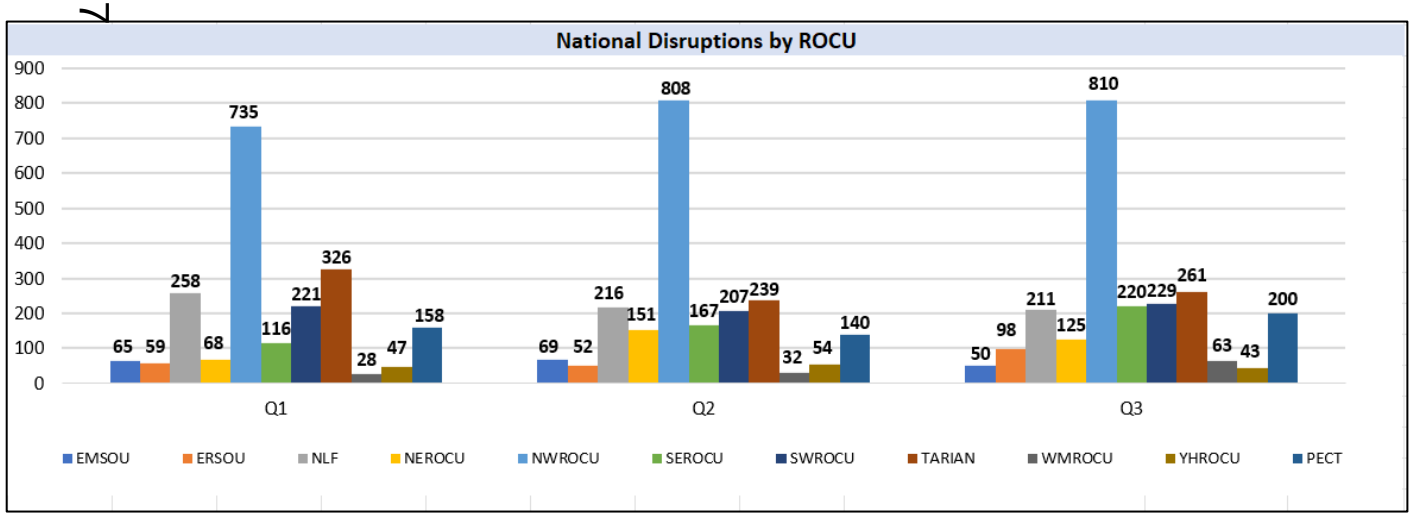
For fraud related disruptions there were:

- **21 major** disruptions - 24% increase (+4) in comparison to Q3 23/24
- **130** moderate disruptions - 25% decrease (-43) in comparison to Q3 23/24
- **2,124** minor disruptions - 49% increase (+703) in comparison to Q3 23/24

Home Office Target Exceeded

F2b For OCG related disruptions, there is a software related issue which is currently in development, and we expect the data to be available for Q4.

Overall, there has been an increase in recording disruptions on APMIS, however the incorrect labelling of the different types of disruptions can cause a skew in the statistics. Ensuring the disruptions are correctly labelled as OCG disruptions can help to mitigate this. CoLP are engaging with all forces and regions to encourage the correct usage of this system.



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

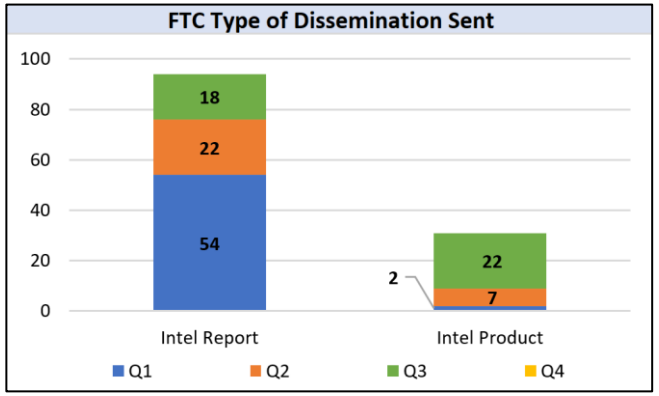
Success Measures:	
F3 Engage in all intensification efforts and target led national operations and evaluate operation-specific outcomes – **Home Office Measure**	⇧
F4 Increase the number of Fraud Targeting Cell packages allocated, adopted and investigated – **Home Office Measure**	⇧

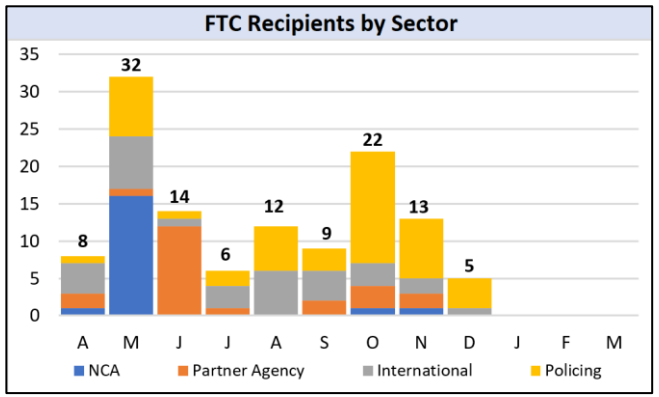
F3 In Q3, **Operation EMMA 10** took place, targeting higher harm individuals responsible for recruiting money mules online (mule herders). Working with private sector partners and The Cyber Defence Alliance, several mule herders were identified operating on Telegram and Snapchat. The operation resulted in **76 arrests, 43 warrants, £818,000 in seizures of cash and cryptocurrency, 13 asset freezing orders and 153 cease & desist notices.** Other seizures included a vehicle, multiple high value mobile devices, bank cards, Class A drugs and approx. 60,000 counterfeit cigarettes.

35 cease and desists were revisited which had been issued during EMMA 9. **No further intelligence had been received of any continued offending**, highlighting the success of the tactic.

In Q4, **Henhouse 4** will take place. which is the annual system wide Pursue intensification on fraud and takes place throughout February. In total, **£763K in bids** have been approved through the NECC led moderation panel, with activity taking place across all 43 police forces, all regions and partners including NCA, FCA and Trading Standards. A comprehensive media strategy is in place to ensure we maximise impact with the public in reassuring victims on the law enforcement response, to deter potential offenders and use the raised profile in the public for protect messaging.

Home Office Target Met





F4 The Fraud Targeting Cell (FTC) is a multi-agency team, comprised of staff from CoLP and the National Crime Agency, and primarily focused on proactive, suspect led intelligence development into the highest harm fraud offenders impacting the UK. The team launched in April 2024 and produce intelligence packages for the National Fraud Squad (NFS) and the wider system.

In Q3, the FTC ran a well-attended **workshop at SOCEX**, leading to future collaborative opportunities with partners. A referral from an external partner about a Ponzi scheme was developed and then taken on by Fraud Operations with multiple arrests taking place, which would not have been possible without utilising the skills and capabilities of both the CoLP and NCA parts of the FTC.

PECT teams made **13 arrests** based on proactive intelligence about mule herders on Telegram. The FTC is also working with Mobile Network Operators on 'sim farms,' with activities planned for the next quarter.

Home Office Target Met

Fraud

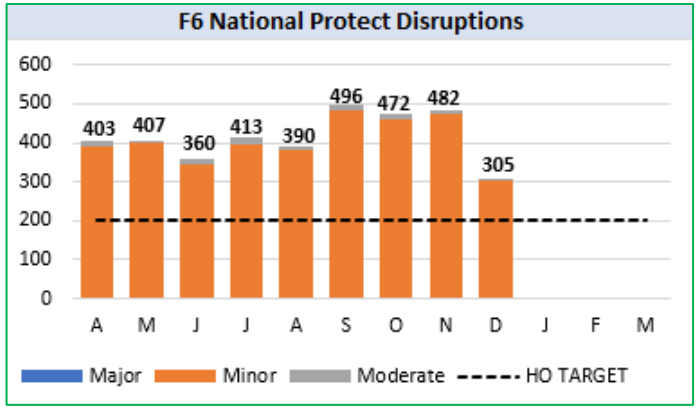
Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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.

Performance Measure 6: 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:	
F5a Increase the number of Protect engagement events and attendees – **Home Office Measure**	⇨
F5b Percentage of protect engagement event attendees (organisations and public) satisfied with the engagement they attended – **Home Office Measure**	⇧
F5c Percentage of protect engagement event attendees (organisations and public) likely to change their behaviours as a result of engagement – **Home Office Measure**	⇧
F6 Increase the number of individuals reached with social media campaigns – **Home Office Measure**	⇧

F5b&c The National Protect Coordinator and their team finalised surveys for protect engagement attendees, and they have been used from the beginning of October. The survey data for the first quarter has been useful in gaining quantitative and qualitative feedback from attendees at events hosted by the National Fraud Protect Network. This enables a full picture of the Network and the work they do to communicate a consistent protect message to the public and organisations, and the behavioural change it encourages. **98%** of attendees were satisfied with their engagement with **96%** likely to change their behaviour. **Home Office Target Met**



F6 In Q3 1,260 disruptions have been reported, an increase by 61% (+477) on the same period of 23/24.

It is expected that this trend will continue as Protect teams become fully staffed and embedded, and forces and regional teams increase recording on APMIS. **Home Office Target Exceeded**

F5a 45 engagements were held across the network, with 184 attendees.

Some local campaigns supported by Protect staff include:

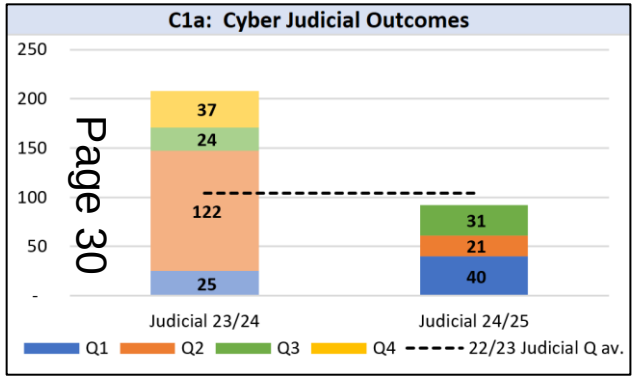
- **NWROCU**: The Fraud Protect Coordinator organized a conference for officers from six North West forces, focusing on the Banking Protocol and the recently implemented PSR. This event provided CPD for the officers.
- **Tarian**: The Protect team presented at the Fintech Wales conference in Cardiff, discussing cyber and fraud prevention and the use of AI. They also participated in Scam Awareness week at the BBC, utilizing the Cyber Van, and were featured on BBC Radio Wales.
- **ERSOU**: The Fraud Protect team worked with universities and colleges, creating new Fraud Protect information packages for Cease & Desist visits as part of Op Emma 10.
- **Met Police:** The team is addressing the theft of mobile phones and subsequent fraud, collaborating with financial institutions, crypto exchanges, and the mobile phone industry.
- **Y&H**: For Op Emma 10, all FE Colleges in the Yorkshire & Humber region were offered briefings for student safeguarding staff on the types of fraud targeting students, including sextortion. A series of meetings and presentations are being conducted across the region.
- **SWROCU**: Fraud Protect achieved the first-ever official major disruption recorded on APMIS in the country. They created an asset pack for Op Emma 10, which included a video, pre-made social media posts, posters, flyers, and still images for digital screens.
- **Home Office Target Met**

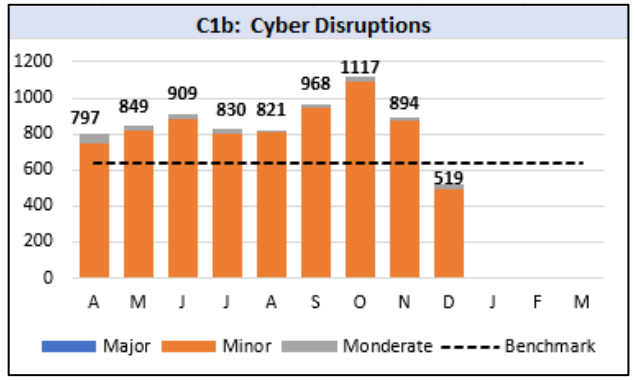
Cyber

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:	
C1a Improve the judicial outcome rate	⇩
C1b Increase the number of disruptions against cyber crime	⇧
C2 Increase the number of operations involving the Computer Misuse Act (CMA)	⇧





C1a Nationally, there have been 31 cyber judicial outcomes during this period and 1,068 non–judicial outcomes. This is a 29% (-7) decrease in comparison to the same period of the previous year. Q2 for 23/24, was a high judicial outcome month with 122 judicial outcomes. Overall, judicial outcomes are reporting a 41% (-64) decrease in comparison to the benchmark for the previous year.

C1b National cyber disruptions are reporting a 25% increase (-510) in comparison to the same period for the previous year. While December figures may be reporting low, overall cyber disruptions have surpassed the benchmark for the entire 23/24 period by 1% (+71).

For Q2 there have been:

- 7 major disruptions - 40% increase in comparison to Q3 23/24 (+2)
- 69 moderate disruptions - 4% increase in comparison to Q3 23/24 (+3)
- 2,454 minor disruptions - 26% increase in comparison to Q3 23/24 (+511)

C2 The Police Cyber Alarm (PCA) pilot expanded in Q3 24/25, distributing Notification Packs to most regions, though not all received Local Malicious IP addresses. A national webinar in January 2025 will launch and distribute Vulnerability and Local Malicious IP Addresses starting February 2025. Officers and staff have welcomed the Notification Packages, recognising PCA's benefits for law enforcement and SMEs. Increased engagement with member organisations has led to initiatives like staff awareness sessions, cyber exercises, and adoption of the NCSC Early Warning Service and CRC core membership. However, a time lag is expected for 'use cases' due to the time taken for subscriber checks on Local Malicious IP Addresses.

The NPCC, partnering with private sector entities, has developed intelligence opportunities to identify UK-based cyber criminals, with a successful proof of concept. Intelligence from third parties is enriched by the NPCC team and forwarded to TICAT for deconfliction and tasking, managed by NCPT and CPDB. Initial intelligence packages are being refined before formalisation, and contracts with intelligence providers are being procured to provide intelligence and expedite the process.

Cyber

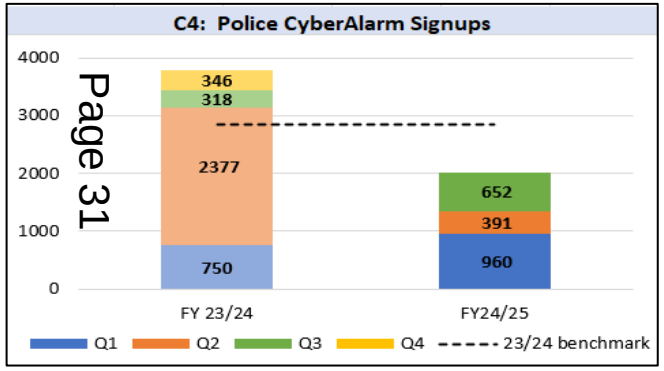
Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

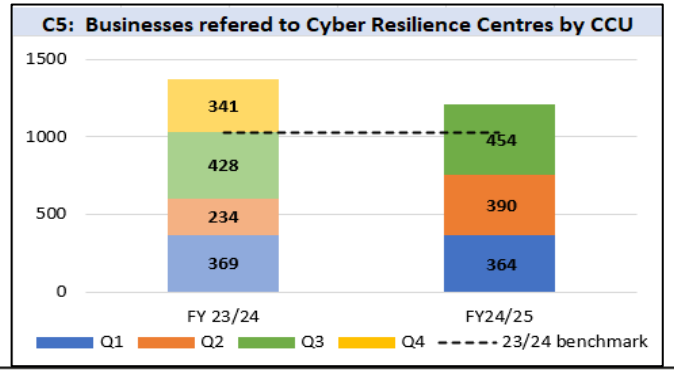
Performance Measure 3: We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.

Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police CyberAlarm 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 CyberAlarm to all SME organisations they engage with.

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:	
C3 Develop the Protect notification procedure and increase notifications issued.	⇧
C4 Protect Officers to promote Police CyberAlarm to SME organisations.	⇩
C5 Increase the number of Cyber Crime Unit referrals to Cyber Resilience Centres.	⇧





C4 In Q3, 652 Small to Medium-sized enterprises (SMEs) signed up to Police CyberAlarm. This is a 67% increase in comparison to Q2, however overall, performance is reporting 30% below the Q3 benchmark (-840). During Q2 23/24 there was a spike in PCA sign ups, this was credited to the Department for Education (DfE) sending out a reminder to schools that membership was a condition of obtaining a Risk Protection Agreement (RPA), essentially commercial insurance. The DfE is an established supporter of Police CyberAlarm, recognising the technical cyber security protection it offers educational establishments that otherwise might not be able to afford specialist IT support.

C5 There has been an increase to the number of Cyber Crime Unit referrals to Cyber Resilience Centres. For Q3, there were 454 referrals made, this is a 6% increase (+26), in comparison to Q3 23/24.
Overall, referrals are reporting 17% (+179) above the 23/24 Q3 benchmark.

C3 In November 2024, an updated operating procedure for the dissemination of three differing types of Protect notifications - Urgent Protect, Protect and Retrospective Protect was introduced. Notifications are sent out by NFIB (unless urgent then directly from source) to the regional Protect teams.

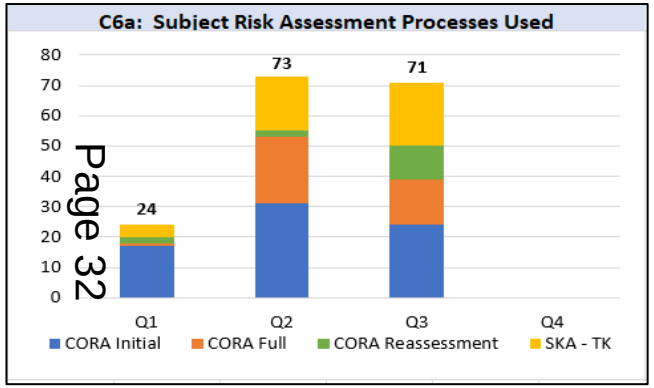
A new KPI has been added to the NPCC Performance Framework for Regional Cyber Crime Units for Q4 24/25: TCUK to complete 100% of NCA Triage, Incident and Tasking (TICAT), or NFIB Protect taskings. This will formalise performance reporting around Protect taskings, 440 had already been sent to the network during Q1-Q3 24/25 using the old operating procedure. Protect Notification outcomes will also be captured, helping to quantify impact of the Protect network; for example, the average ransomware payment is assessed to be £1.75 mill (NAC assessment) therefore each successful Protect intervention could be said to save UK businesses such an amount.

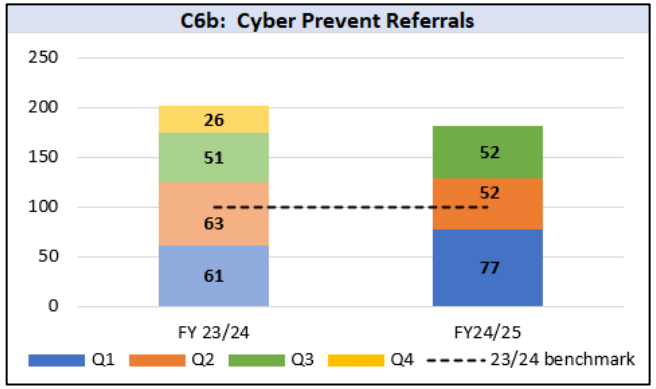
Cyber

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 PREVENT referrals.
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.

Success Measures:	
C6a Increase the number of CORA assessments made	⇨
C6b Increase the number of PREVENT referrals	⇧
C7 Increase the number of CDSV Programme participants and their utilization across the network.	⇧





C6a Cyber Offending Risk Assessments (CORA) consolidate threat, vulnerability, and impact data to equip decision makers with actionable intelligence for securing their cyber infrastructure. The number of risk assessments using this process decreased from Q2 to Q3 from 46 to 42, a decrease of 3% (-4). Q2 & Q3, however have shown a large increase in comparison to Q1.

C6b **Please note this data is for October and November only*. A total of 52 Cyber Prevent referrals were received in Q3 down 2% (-1) from Q2 the previous year. There has been an improvement on the 23/24 quarterly average of 50 referrals, which has been met in Q3. The measure appears on track to improve upon last year's total.

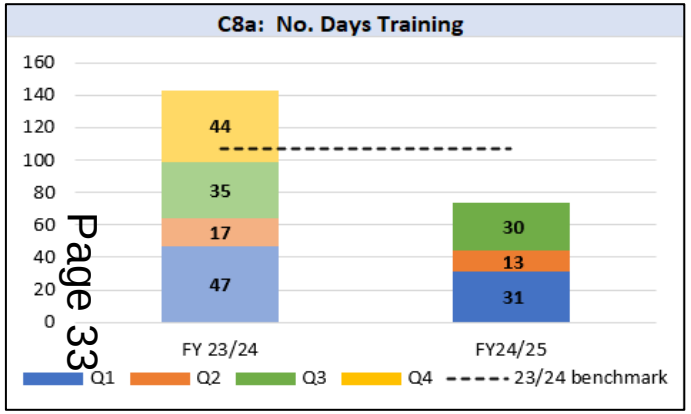
C7 In Q3, ten volunteers joined across six different force or regional teams, bringing the total to 128 across 33 teams. The volunteers remain primarily in the cyber network, although work has expanded into fraud, economic crime and wider SOC. The value of volunteering was recognised by nominations for outstanding CDSVs and CDSV managers for NPCC Cybercrime Commendations throughout Q3.
Activities in Q3:

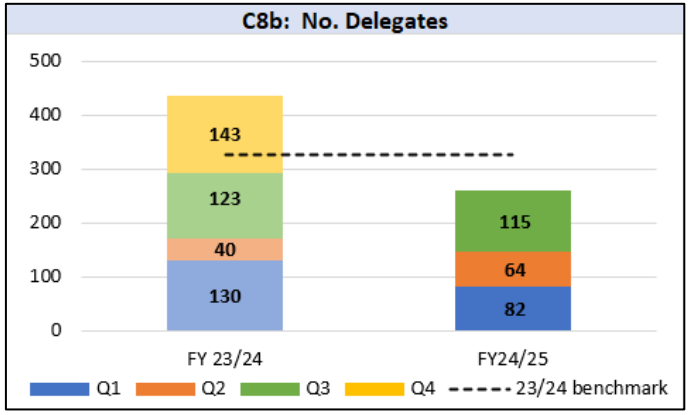
- AI generated audio detection project - engagement with Home Office innovation and research on new applications for voice alteration
- Delivery of Cyber escape rooms/exercises at various locations
- Dark Net Market monitoring and intelligence generation
- Guest lecture on AI and Crime at the University of Portsmouth
- AI training delivery to Merseyside Police ECU
- Cyber Protect and Prevent presentation to parents of schoolchildren
- Project to provide automated systems to monitor activity and performance recording for POLIT and Cyber.
- Assistance with reviewing and further developing python scripts written by NYP Cybercrime.
- Op Tipper taskings (OSINT for high-risk stalking cases)
- Workshop input to 19 second year business students concerning the application of data security topics.

Cyber

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:	
C8a Increase the number of Cyber training days	⇩
C8b Increase the number of Cyber training delegates	⇩





C8b The number of delegates followed a similar seasonal pattern to 2023/24, with Q3 reporting an 80% increase (+51). In comparison to Q3 for 23/24, there is a 7% decrease (-8) in training delegates.

SudoCyber is a gamified learning platform where access is provided to officers and staff across TCUK by NPCC Cybercrime to support initial learning and ongoing CPD. SudoCyber contains multiple short training modules called labs covering a variety of areas across the 4Ps. For Q3, SudoCyber has seen a 10% increase in the completion of training labs.

The NPCC Cybercrime Team is now using AccessPlanit (the same platform as ECCA). In populating the cyber resources on the platform, the NPCC Team can now review and understand the capacity of the networks. The ability for regions and forces to book their own courses is now expected to go live in February 2025.

C8a During Q3, 30 days of training were delivered to 115 delegates. The number of courses has increased in comparison to Q2 by 131% (+17), however it was noted in Q2, there is often a seasonal dip in the second quarter. In comparison to Q3 for 23/24, training days are reporting a 14% decrease (-5).

This page is intentionally left blank

City of London Corporation Committee Report

Committee(s): Economic and Cyber Crime Committee	**Dated:** 4 February 2024
Subject: Cyber Griffin Update	**Public report:** For Information
This proposal: • **delivers Corporate Plan 2024-29 outcomes** • **provides statutory duties** • **provides business enabling functions**	CoLP impact the following Corp Plan outcomes: Vibrant Thriving Destination- (Community Safety/ CT) Dynamic Economic Growth- (National Lead Force)
Does this proposal require extra revenue and/or capital spending?	No
If so, how much?	£-
What is the source of Funding?	N/A
Has this Funding Source been agreed with the Chamberlain's Department?	N/A
Report of:	The Commissioner
Report author:	Charlie Morrison, Helen Thurtlesmith

Summary

In both Q2 and Q3, Cyber Griffin exceeded its quarterly targets placing the programme in a very strong position to end the financial year (FY) with all targets achieved. Forecasting suggests that Q4 will produce record engagement for this time of year. Considering the staffing challenges during the year, the programme is very positive about these returns.

Over the next period, Cyber Griffin will evaluate its strategic targets for the coming FY and review its service offering with the aim of establishing how the programme will continue to grow and further develop its impact in the FY 2025/26.

In the previous meeting the committee asked detail on what was meant by the 'record number of services' and commented that the programme's reporting focuses on activity over impact. These topics are addressed in the report.

Recommendation(s)

- Note the report.

Main Report

Background

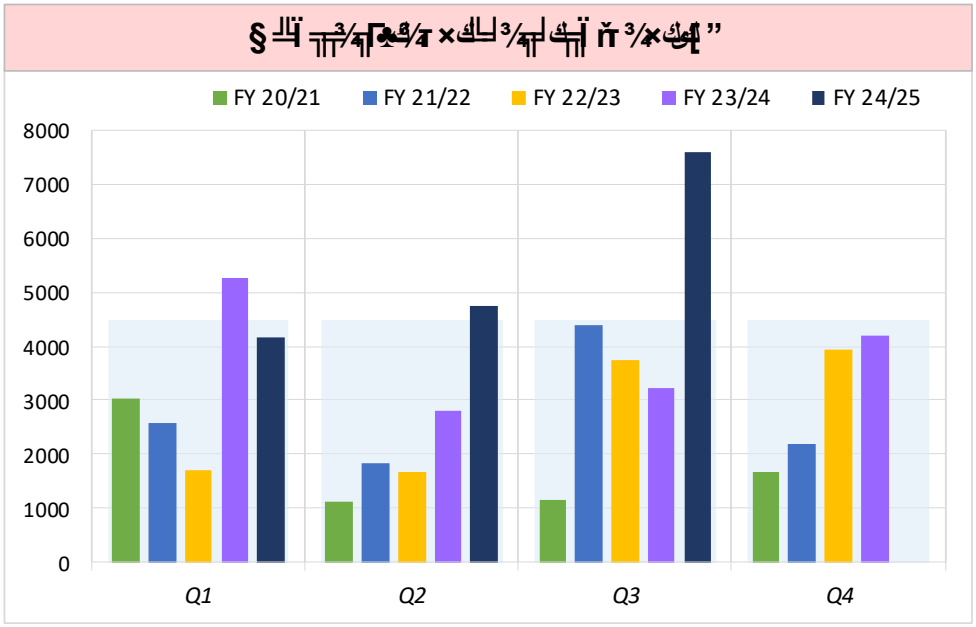
This report gives a brief update on the current position of the Cyber Griffin programme. For details of all Cyber Griffin services please visit: www.cybergriffin.police.uk

Current Position

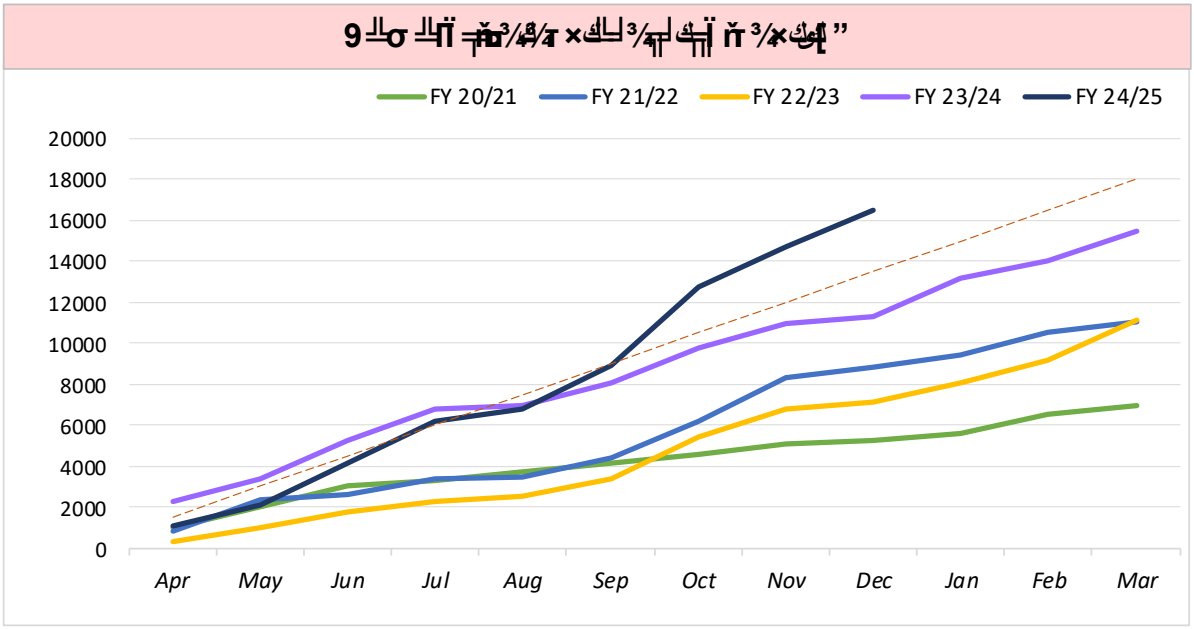
1. Cyber Griffin trained 7,596 end users in Q3. This was 169% of the quarter's target of 4,500.

2. When the programme uses the term 'record numbers', this refers to measuring current performance against performance over the same period in previous years. The programme currently has five financial years of data to compare, as the graphs demonstrate.

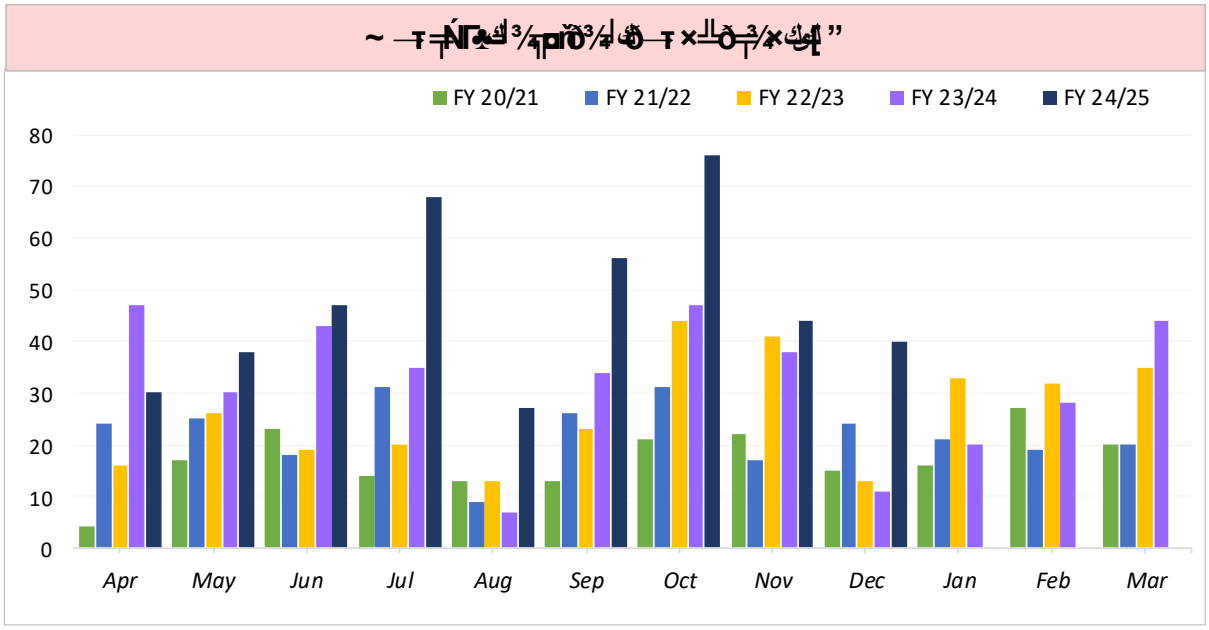
Graph showing Cyber Griffin's cumulative end users trained over five financial years.



Graphs showing Cyber Griffin's quarterly users trained compared over five financial years.



Graph showing the number of Cyber Griffin services delivered over five financial years.



3. Regarding locally set targets, in Q3, the programme trained 7,596 people (quarterly target of 4,500), conducted 160 services (quarterly target of 100) and partnered with 53 new client organisations (quarterly target of 50).

4. Regarding performance against national targets, Cyber Griffin continues to meet all nationally set key performance indicators (KPIs). Specifically, the programme has engaged with 100% of victims of cyber-dependent crime.

Survey data also demonstrates that engagements create security behaviour changes in above 75% of delegates. The same events have a satisfaction rate of considerably above 75%.

5. Measuring impact over activity is challenging in PROTECT work. Quantifying crimes that were avoided, measuring security improvement, and capturing security behavioural change requires longitudinal qualitative assessment. This approach further requires the long-term support of organisations who agree to be measured. In addition to tracking activity and quality assuring the veracity of its service offering through external assessment led by the NCSC, Cyber Griffin does measure this area in a limited way through survey feedback and testimonials.

   1,345 surveys have been received so far over the current FY which equates to approximately 8% of delegates trained despite surveys being offered at the end of every delivery. Responses are overwhelmingly positive. An example of some questions and the responses received are detailed in the table.

Question	Response
Following this event, how likely would you be, if at all, to change any of your personal online/ security behaviours?	86% said 'likely'
To what extent has this training improved your confidence in your cyber security?	48% said 'a lot' 40% said 'a fair amount'
How relevant to you personally, if at all, did you find the topics covered during the engagement/event?	79% said 'very relevant' 20% said 'relevant'

   Additionally, the programme receives testimonials. This FY these have included:

   "This was a very insightful presentation. The presenters were articulate and very effective in conveying their message."

   "Best webinar I have attended, ever!"

   "The police service is well aware of cyber security risks and wish to protect the public."

   "Very clear and concise with good explanations of what can be complex areas. Really set me thinking about what measures I already have in place and what could be improved."

   "This is well worth watching even if you are something of a computer wizard."

"This was genuinely one of the best presentations I have seen in a long time. Useful, vital information about security with clear explanations of the risks and practical suggestions for measures to improve security."

"An excellent overview of current cyber threats and practical steps that can be taken to mitigate against them."

All the qualitative feedback was provided immediately following deliveries. The team's experience and cyber security doctrine both heavily endorse that effective training is critical to protecting individuals and businesses from cyber attack. Unfortunately, the programme currently does not have the capability to return to delegates to measure lasting impact.

In the coming period, Cyber Griffin aims to investigate whether longitudinal qualitative measurements can be conducted in a resource effective manner.

6. Cyber Griffin's financial situation is strong, but it should be noted that a review will be needed prior to the FY 2025/26. The programme has confirmed both the Corporation Business Levy and NPCC Cyber Crime Programme funding. Additional costs were incurred however due to the recent officer and staff pay rises from the FY 24/25. As funding streams are fixed, they do not consider year on year financial increases to salaries and professional fees. A costs review is being conducted and may result in a requirement for an uplift in funds to deliver the current service offering.

Conclusion

7. Cyber Griffin is enjoying a very strong period of performance and forecasts to end the financial year having delivered on its national and local targets. Cyber Griffin's financial position is being reviewed and will be reported on in the next meeting. Over the next period, the programme will evaluate its strategic targets for the coming financial year and review its service offering with the aim of establishing how the programme will continue to grow and further develop its impact in the FY 2025/26.

Report Authors:
Inspector Charlie Morrison
Head of Cyber Griffin, Cyber Crime Unit, Specialist Operations Directorate
E: Charlie.morrison@cityoflondon.police.uk

Helen Thurtlesmith
Project Manager
E: Helen.thurtlesmith@cityoflondon.police.uk

This page is intentionally left blank

Committee(s): Economic & Cyber Crime Committee	**Dated:** 04/02/2025
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: Senior Policy and Innovation Adviser, Innovation & Growth	Elly Savill

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.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime, as well as cross-team working between IG and the City of London Police (CoLP) since the Economic & Cyber Crime Committee (ECCC) last convened in November 2024. The report provides an update on IG's Artificial Intelligence (AI) Innovation Challenge, a new cybersecurity talent initiative and ongoing work on digital verification.

Links to the Corporate Plan

The activities set out in this report help deliver against the Corporate Plan's outcome to support dynamic economic growth. Specifically, ensuring that the City has the safest, most secure business environment in the world and promoting the UK as a place that is open, innovative, and sustainable.

Main Report

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

1. We continue to use this report to highlight those activities which demonstrate the benefits of IG and CoLP collaboration to make the UK the safest place in the world to do business. IG continues to look for ways to promote the activity of CoLP and support their work as part of our wider stakeholder engagement.

Collaboration

2. IG was delighted to welcome Oliver Shaw, Temporary Commander for Fraud and Cyber Crime at the CoLP, to speak at the AI Innovation Challenge Showcase event. IG felt it was important to have the CoLP represented at the event, to highlight their role as National Lead Force for fraud and the National Police Chiefs' Council lead for economic and cyber-crime. CoLP also provided the important context for how AI is impacting online fraud and the need for collaboration and innovation to safeguard businesses and customers.

AI Innovation Challenge

3. At the previous Committee meeting, Members received an update on the AI Innovation Challenge. The Challenge brought together ten innovative technology companies and eight large FPS firms to collaborate across a seven-week sprint. Participants engaged 1:1 to develop and accelerate solutions which answered the use case: *How can AI prevent online fraud at the earliest possible stage by identifying and tracking fake identities - including synthetic identities and image or audio deepfakes?* Participants benefitted from input and expertise from our supporting partners - Microsoft, NayaOne the Department for Business and Trade (DBT), and London and Partners.

4. IG have previously delivered two Cyber Innovation Challenges. The 2024 AI Innovation Challenge followed a similar format and objectives to these Challenges but was more ambitious in scope. Compared to the 2023 Challenge, we welcomed an additional six FPS and tech participants, held 80 1:1 meetings between participants (+26) and nine collaboration sessions (+3). As well as this, through our partnership with NayaOne, the AI Innovation Challenge offered exclusive access to a secure sandbox environment and relevant data sets for the tech participants to test their solutions throughout the sprint stage.

5. On 4th December 2024, the Challenge concluded with a public showcase event at Guildhall. The event supported around 100 attendees from across the private sector, regulators, government departments and academia. Attendees heard from the Policy Chairman and senior representatives from Microsoft and the CoLP. There was also a panel discussion with participating FPS and tech firms, as well as a presentation of several tech solutions developed and enhanced across the sprint and in response to the use case.

6. Initial findings from the Challenge have been positive:
   - Almost half of the tech firms said that participating had accelerated product development by three months, with one tech firm saying nine months.

- Many of the tech participants confirmed that the Challenge allowed them to validate their solutions and gain valuable insights from the financial services sector.
- 100% of the participating FPS firms achieved what they wanted to from the Challenge which included a better understanding of technology developments in this space and a chance to share advice and learnings with the tech participants.
- 100% of the participating FPS firms plan to continue engagement with at least one of the tech companies from the Challenge.
- 95% of all participants would recommend participating in the Challenge.
- 100% of tech firms confirmed that participating in the Challenge had improved their understanding of the needs of FPS firms.

7. At the previous Committee, members were interested to understand how IG had engaged with the media and communications teams to raise the profile of the Challenge. A summary of this engagement and the outcomes is as follows:

Month	Engagement / outcome
May 2024	• Press release to announce AI Innovation Challenge in partnership with Microsoft
June 2024	• AI Innovation Challenge referred to in the Lord Mayor's speech at the Science and Innovation banquet
	• Talking heads filmed with the Policy Chairman and past Innovation Challenge participants to raise profile of AI Innovation Challenge
June - July 2024	• Talking heads post to announce tech applications open • Tech application announcement shared by supporting partners and member organisations across social media and newsletters
July 2024	• Personalised graphics created for firms to announce their participation on social media (example here)
August 2024	• Global City webpage updated with confirmed FPS and tech participants
November 2024	• Digital certificate of participation created for FS and techs to share on social media and websites
December 2024	• Social media post for showcase and updated Global City webpage • Press release and Policy Chairman's talking heads clip • Policy Chairman's CityAM column highlights the AI Innovation Challenge
January 2025	• Talking heads clips with participants shared on social media

8. Looking ahead, IG will evaluate feedback from Challenge participants to identify the key wins and areas for improvement. IG will also contact all participants in six months to identify the long-term impact of the Challenge.

9. IG is unlikely to hold an Innovation Challenge for 2025. However, the team will continue to work closely with FPS and the tech sector to nurture innovation and support the adoption of tech solutions which address the needs of FPS.

Digital Verification

10. The City of London Corporation's hallmark *Vision for Economic Growth (2023)* report identified acceleration of Digital Verification (DV) solutions across FPS as a significant opportunity for the UK economy. The government estimates that widespread adoption of DV solutions could deliver potential £4.8bn in value added from 2024 - 2030, with a significant proportion of this reflecting the mitigation of fraud losses.

11. In this context, IG is focusing on the UK's DV infrastructure offer to boost adoption, drawing on the experiences of strategically important global markets. Our work encompasses both the verification of corporations and individuals.

12. In 2023, the City of London Corporation and HM Treasury co-founded the Centre for Finance, Innovation and Technology (CFIT) - providing a combined £5.5m seed investment. CFIT exists to unblock barriers to FinTech market growth. The creation of CFIT was a recommendation of the *Kalifa Review of UK FinTech (2021)*.

13. CFIT's current, ongoing Coalition is focused on catalysing verification of corporates. IG is supporting this through provision of resource in the form of its Senior FinTech Policy Adviser on partial secondment to CFIT. IG is also leading on work on individual verification. Two private industry roundtables have been held, with input from HM Treasury, the Department for Science, Innovation and Technology, and the Department for Business and Trade. These included C-level and director-level from the largest banks and FinTechs in the UK, the CEO of CFIT, and Baroness Swinburne. The first roundtable took place on 25 July and the second took place on 28 November. The roundtables have informed research undertaken by IG, as we continue to compare jurisdictions and understand which form of individual DV infrastructure is viable for the UK.

14. More detailed recommendations on scaling DV solutions from IG (for individuals) and CFIT (for corporates) will be forthcoming in two separate reports published in Q1. The audience for both reports will be government, regulators and industry, with both likely to include recommendations to be taken forward by these stakeholders.

Cybersecurity Talent initiative

15. The IG Skills and Workforce Policy Team is in the process of scoping a new national skills programme to increase the size of the UK's cybersecurity talent pool. Research indicates that there is a clear need for increasing the number of skilled cybersecurity professionals so that businesses can enhance their resilience to cyber-attacks in the UK's FPS sector, including for small and medium-sized businesses.

16. This new programme is scheduled to be fully scoped and delivered in April 2025 and is subject to Policy & Resources Committee's approval of the IG business plan.

17. One report which identifies this talent need is the UK Government's Cyber Security Skills in the UK Labour Market 2024. This found that 8,100 individuals

entered the UK cyber security workforce in 2023, leaving an estimated shortfall in 2023 of around 3,500 people. Moreover, the report found that 44% of businesses have basic technical skills gaps, and 27% have advanced skills gaps.

18. As part of the scoping phase for the new cybersecurity talent programme, the Skills and Workforce Policy team has engaged with experts in the CoLP and the City Corporation's SME Strategy. The team is now identifying other relevant stakeholders to engage with, to explore some potential impactful interventions which the City Corporation could pursue to drive measurable change in this policy area.

Corporate & Strategic Implications

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

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

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

22. Legal implications - None identified for this paper.

23. Risk implications - None identified for this paper.

24. 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 City Corporation's EDI commitments.

25. Climate implications - None identified for this paper.

26. Security implications - None identified for this paper.

Conclusion

27. Although the AI Innovation Challenge has now concluded, in 2025 IG will continue to engage on economic crime and cyber through initiatives such as our work on digital verification and cyber talent. We will also continue to engage with CoLP in relation to their national lead force role, utilising the force's briefing in our own engagement with relevant external stakeholders (including, but not limited to, financial services firms).

Elly Savill
Senior Policy and Innovation Adviser
Innovation & Growth
T: +44 (0) 7500 785073
E: eleanor.savill@cityoflondon.gov.uk

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank