CITY OF LONDON POLICE
National Policing Lead For Fraud

National Lead Force
National Delivery Plan Performance Report

Q2: July – September 2024

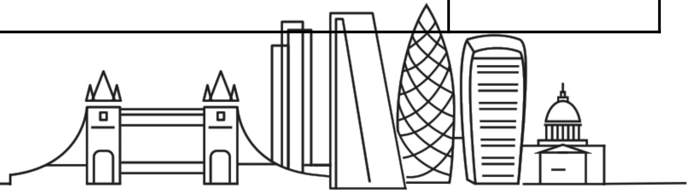
A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

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

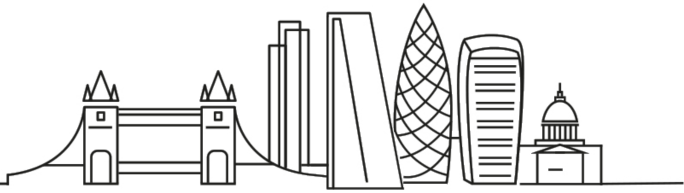
MLAR 1	We will increase criminal justice outcomes and disruptions against money laundering offenders.	⇩
MLAR 2	We will seize and restrain more criminal assets through including released asset denial activity	⇧
MLAR 3	We will provide training to policing on how to investigate and seize crypto assets. 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.	⇨
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.	⇧

CITY OF LONDON POLICE



Performance Assessment

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

Proactively pursue offenders.

- MLAR asset seizures valued at £15,061,701
- £1,863,192 in Cryptocurrency seizures
- 2,041 disruptions for Fraud, 26 were Major
- No intensification, but national operation
- The FTC sent 29 intel disseminations

Improve outcomes for victims.

- 10 judicial reviews were recorded for MLAR
- 1,162 MLAR disruptions including 44 Major
- NFIB disseminations increased by 63% (+3,876)
- 35% (+497) increase in Fraud judicial outcomes
- 10% reduction in outstanding disseminations
- 21 Cyber judicial outcomes
- 5,864 disruptions for Cyber, 74 were Major
- CyberAlarm notifications trial launched in Oct
- Cyber training fell by 23%, a seasonal pattern

Protect people and businesses from the threat of fraud, economic and cyber crime.

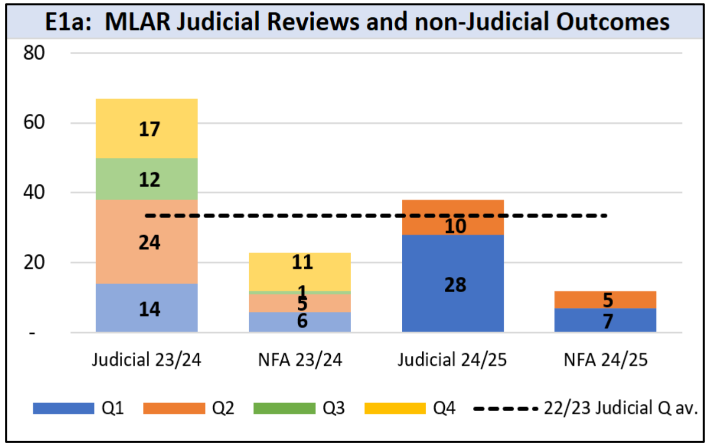
- Protect teams supported 5 campaigns
- 1,162 Fraud Protect disruptions
- Cyber Protect notification pack to launch
- 391 new SMEs signed up to CyberAlarm
- 500 referrals to Cyber Resilience Centres
- 175% increase in CORA reviews
- 52 Cyber Prevent referrals received
- 20 CDSVs in 15 forces were active

Money Laundering and Asset Recovery

Improve Outcomes for Victims

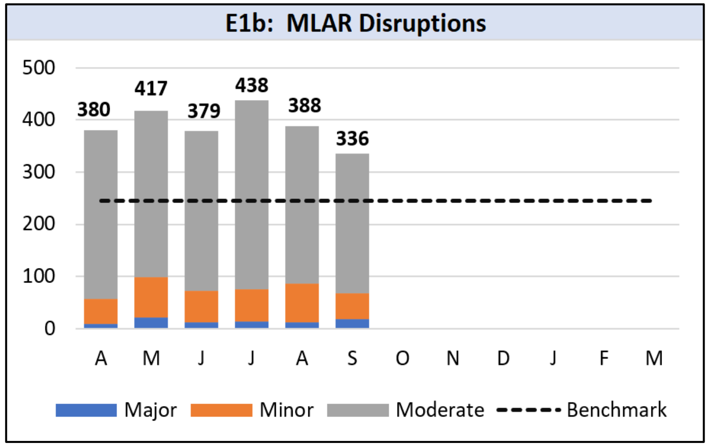
Performance Measure 1: We will increase criminal justice outcomes and disruptions against money laundering offenders.

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



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 arrests and outcomes. These are now counted as Judicial Reviews through the measures of Charged and NFA.

For Q2, 10 judicial reviews were recorded, this is 58% (-14) decrease compared to Q2 for the previous year. The yearly total of 38 judicial reviews is 12% (+4) above the benchmark target from 23/24.



E1b Money laundering and asset recovery is classed as illicit finance on APMIS. In Q2, there were a total of 1,162 disruptions.

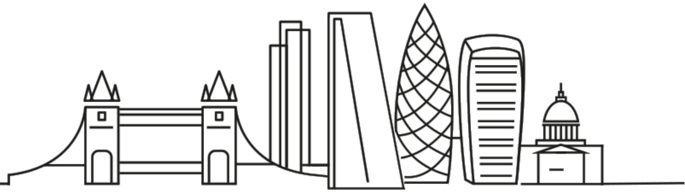
- 44 major (31% increase (+10) in comparison to Q2 23/24)
- 186 moderate (55% increase (+66) in comparison to Q2 23/24)
- 932 minor (151% increase (+561) in comparison to Q2 23/24)

The benchmark from 23/24 was 2,940, which translates to 735 disruptions per quarter. For Q2, disruptions are 58% (+427) above the benchmark target. Overall, a positive quarter for disruptions.

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.

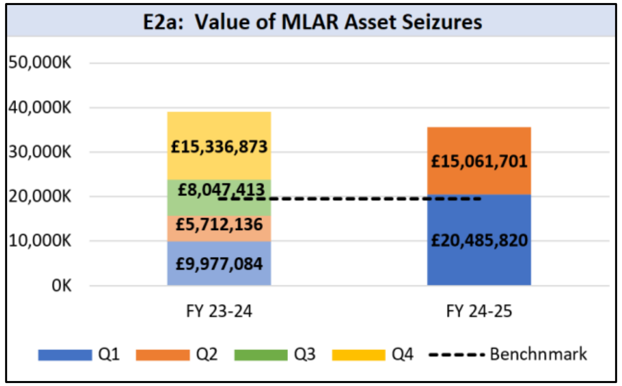


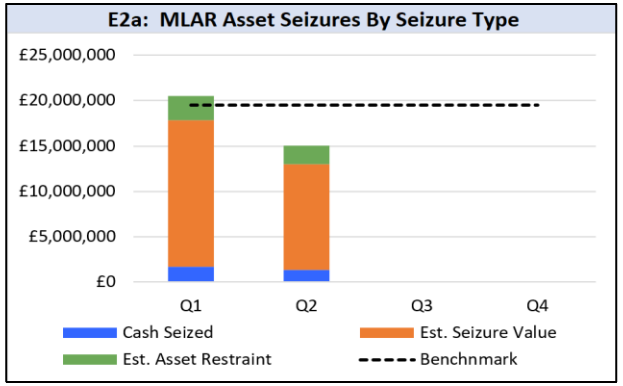
Money Laundering and Asset Recovery

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.	N/A
E3 Recover a higher number of crypto assets.	⇧

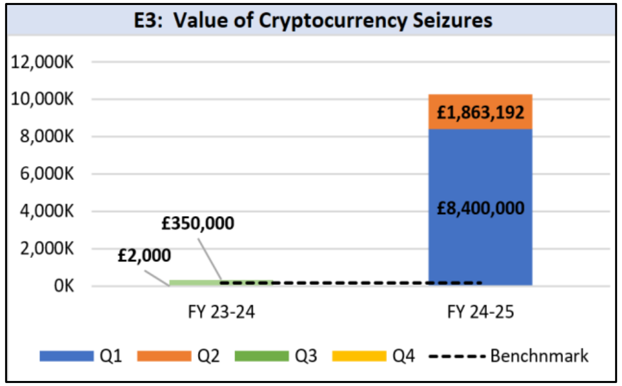




E2a In Q2 a value of £15,061,701 asset seizures were recorded for money laundering and asset recovery. This is a 90% (+£9,349,565) increase from the same period in 23/24, and 23% (+£4,475,052) above the 23/24 quarterly average.

A breakdown of the seizure types shows estimated seizure value accounted for 77% of all seizures for Q2. For the previous year estimated seizure value was the highest occurring seizure type at 90%. The types of asset seizures can vary depending on the operation or intensification occurring within that period.

E2b Currently, there are no outcomes available for civil recovery orders on APMIS. This is likely an entry issue and has been raised for discussion.



E3 For Q2, there has been £1,863,192 in cryptocurrency seizures. The quarterly benchmark for this quarter is £78,636 and Q2 is reporting 12,952% above this (+£10,184,556). This increase can be explained by the new powers that came into force this year for crypto asset seizures.

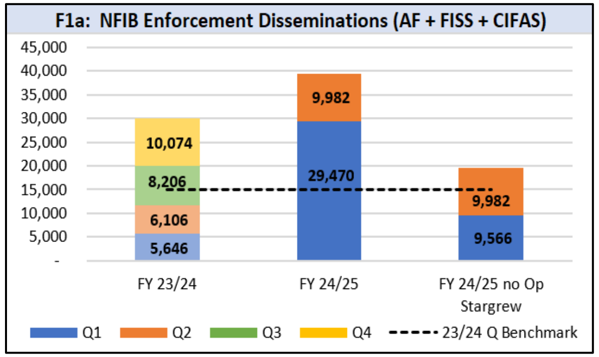
It is believed that all ROCUs are seizing crypto assets, and in the last year ROCUs have also corrected some input errors on APMIS, inflating the 24/25 figures in comparison to 23/24. The NWROCU reported a single seizure of £680k+ in Q2.

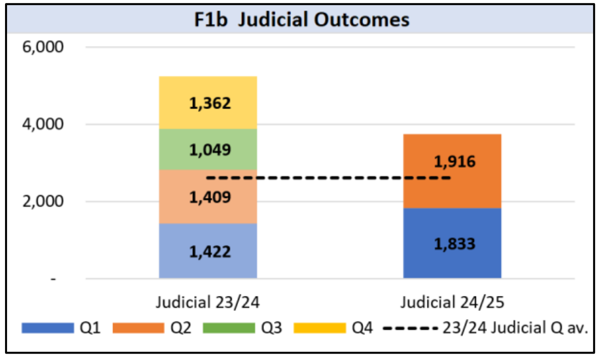
Fraud

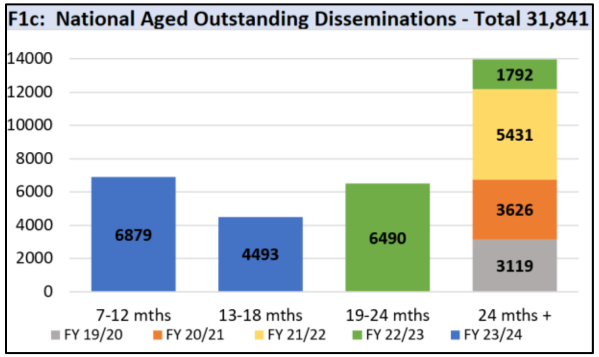
Improve Outcomes for Victims

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).	⇧
F1b Improve the judicial outcome rate and the alternative positive outcome rate.	⇧
F1c Reduce the percentage of outstanding returns.	⇩







F1c For aged outstanding disseminations, data up to September 2024 reports 44% (31,841) of disseminations are marked as outstanding for England and Wales.

In comparison to Q1 24/25, this is a 10% reduction (-3,320).

F1a NFIB disseminations increased in Q2 by 63% (+3,876) in comparison to Q2 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 is reporting figures are closer to normal range, however still considerably larger than the previous year's average.

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 1,916 judicial outcomes during this period and 10,064 non–judicial outcomes. This represents a 35% (+497) increase in judicial outcomes in comparison to the previous year. NFA outcomes have decreased by 3% (-346) in the same period. The high levels of outcomes in Q2 24/25 are driven by two large cases returning large numbers of outcomes.

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

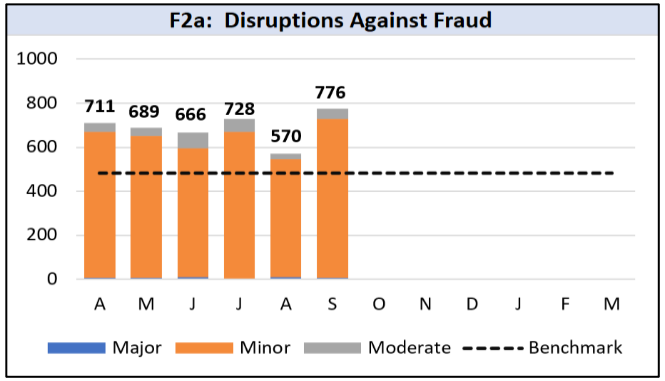
Fraud

Proactively Pursue Offenders

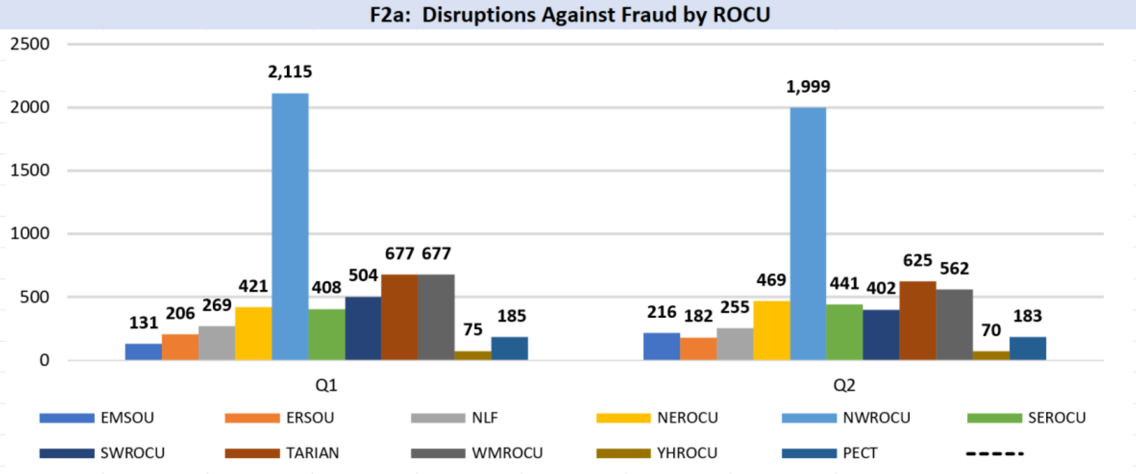
Performance Measure 2: We will deliver and co-ordinate regional Proactive Economic Crime Teams and uplifted National Lead Force teams to form part of the National Fraud Squad. The NFS teams will proactively target fraudsters and disrupt offending achieving criminal justice and alternative outcomes.

Success Measures:	
F2a Increase the number of disruptions against Fraud.	⇧
F2b Increase the number of disruptions against Fraud organised crime groups (OCGs).	N/A

F2a: Disruptions Against Fraud



F2a: Disruptions Against Fraud by ROCU



F2a Nationally there were 2,074 disruptions recorded for Q2. This is 43% above the current benchmark for 23/24 (+1246).

For fraud related disruptions there were:

- **22 major** disruptions (5% increase (+1) in comparison to Q2 23/24)
- **128** moderate disruptions (36% decrease (-73) in comparison to Q2 23/24)
- **1,924** minor disruptions (111% increase (+1,014) in comparison to Q2 23/24)

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 Q3.

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.

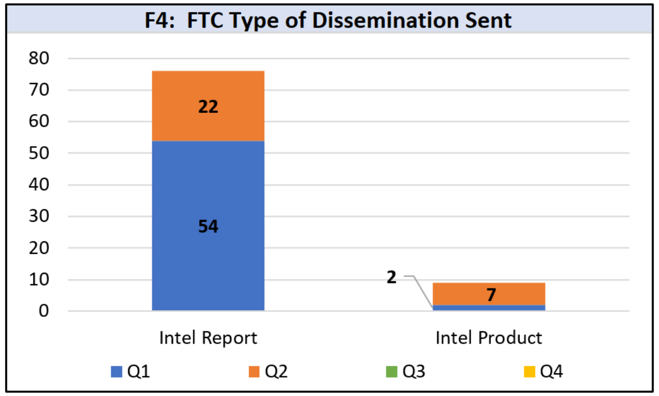
Performance Measure 4: We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations

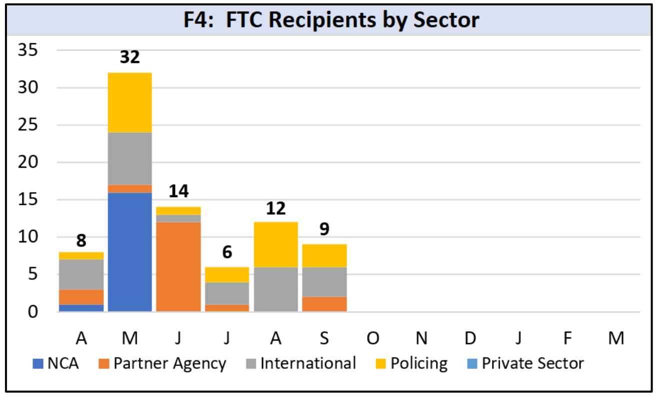
Success Measures:	
F3 Engage in all intensification efforts and evaluate operation-specific outcomes, including arrests, disruptions, asset seizures, and charges.	⇩
F4 Increase the number of fraud targeting cell packages allocated, adopted and investigated.	⇩

F3 There was no national NECC led intensification scheduled for Q2. The next intensification period will be in November and is named Op EMMA 10. This will be a national intensification targeting money mules. During Q2 13 intelligence and evidence packages have been built in preparation and distributed by the Intelligence Development Team to the Regional Proactive Economic Crime Teams.

In Q2 the NCA led a national investigation, Op Neogamy, into a criminal service used to ‘spoof’ phones to commit fraud. It allowed fraudsters to socially engineer victims into believing they were speaking to a company, such as a financial institution. The estimated number of UK victims is over 170,000 and of those who reported to Action Fraud, the average loss is over £9,400.

The NCA identified users of this service and sent intelligence packages to PECT teams for investigation. CoLP teams have checked nearly 100,000 entities of identifiable information on the NFIB database and Action Fraud system, providing grounds for research gathering and analysis that will go toward intelligence packages, and further prevention and disruption.





F4 The Fraud Targeting Cell (FTC) is a multi-agency team, currently comprised of staff from City of London Police and the National Crime Agency, 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 the second quarter since the team launched, there have been numerous presentations made to the ROCUs and private sector. The team received 18 referrals in relation to Telegram handles believed to be engaged in money mule herding activity, and development work began to produce packages to disseminate to the PECTs as part of the Op Emma 10 intensification against this fraud type.

In Q2, 38 Referrals were received, and 29 intelligence disseminations were sent out by the team. Of these disseminations, one was sent internationally, one to the Met, and three were referred to the London PECT.

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.

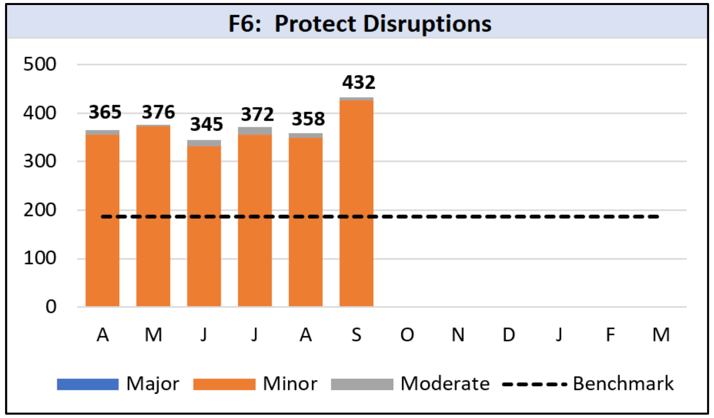
Performance Measure 6: We will deliver agreed and consistent content across the PROTECT network, to ensure consistent messaging in line with HMG guidance and promoting HMG systems and services.

Success Measures:

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

F5b&c The National Protect Coordinator and their team have finalised the surveys and they were sent out to the Regional Fraud Protect Coordinators at the beginning of October. Some data should be available for the Q3 report.

PROTECT teams' recruitment is complete in eight Regions. The two regions still under recruitment are South East and the Metropolitan Police Service. Teams have supported five national campaigns this quarter including holiday fraud, student awareness, pension and ticket frauds and the NECC's next intensification, along with Action Fraud campaigns.



F6 In Q2 1,162 disruptions have been reported, this is an increase by 173% (+737) in comparison to the same period of 23/24.

It is expected that this trend will continue as the Protect teams become fully staffed and embedded, and as forces and regional teams increase their recording on APMIS.

F5a Some local campaigns supported by Protect staff include:

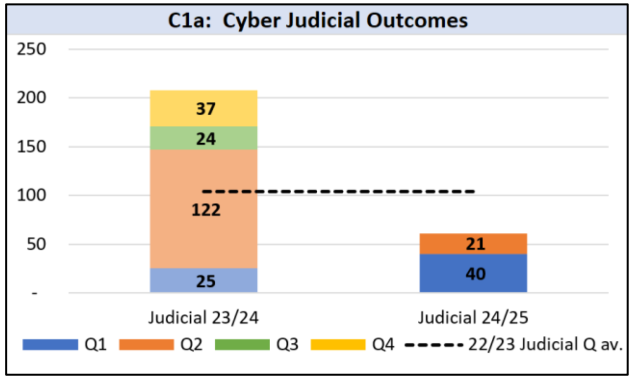
- **NWROCU** – The North West Fraud Protect Conference is being held at the University of Central Lancashire with delegates also coming from the Midlands and Yorkshire. Estimated protect officers in attendance are 20 to 25.
- **TARIAN** – A project has been designed to upskill SMEs in the region on bribery and corruption. Two large Eventbrite sessions have been arranged for October, and as part of this there will be a focus on the "Thatscorruption" site, including the quiz.
- **All Regions** – In support of Op Emma 10, all regions are engaging with their universities to try and prevent students becoming money mules. This follows their recent work during freshers' weeks trying to prevent fraud against students.
- **Met Police** – Focused on presentations on high harm areas of courier and romance fraud. They have also started a joint project with West Midlands ROCU and CoLP's National Protect Coordinators Office to design and deliver romance fraud prevention and awareness videos.

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)	⇧

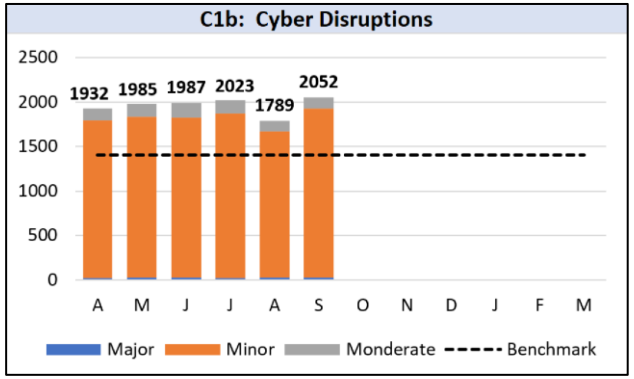


C1a Nationally, there have been 21 cyber judicial outcomes during this period and 1,186 non–judicial outcomes. This is an 83% (-101) decrease in comparison to the same period of the previous year. Q2 for 23/24 was a high judicial outcome month with 122 judicial outcomes. Overall, judicial outcomes are reporting a 41% (-43) decrease in comparison to the benchmark for the previous year.

C1b National cyber disruptions are reporting a 65% (+2,316) increase in comparison to the same period for the previous year, and a 39% increase against the benchmark for the previous year.

For Q2 there have been:

- **74 major** disruptions (15% increase (+11) in comparison to Q2 23/24)
- **390** moderate disruptions (67% increase (+26) in comparison to Q2 23/24)
- **5,400** minor disruptions (43% increase (+2331) in comparison to Q2 23/24)



C2 Police CyberAlarm (PCA) is developing the processes and procedures to send proactive notification packages out to regions and forces. It is currently being piloted in the NEROCU and SEROCU from October 2024, whereby the regions receive two types of notification packs (vulnerability and local malicious IP addresses) through the PCA Dashboard with the intention to generate Pursue or Prevent opportunities. The aim is to roll this out nationally in February 2025.

Region	Notification Pack Type	Amount Allocated
NEROCU	Malicious Activity	13
NEROCU	Vulnerability	2
SEROCU	Malicious Activity	21
SEROCU	Vulnerability	8

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.

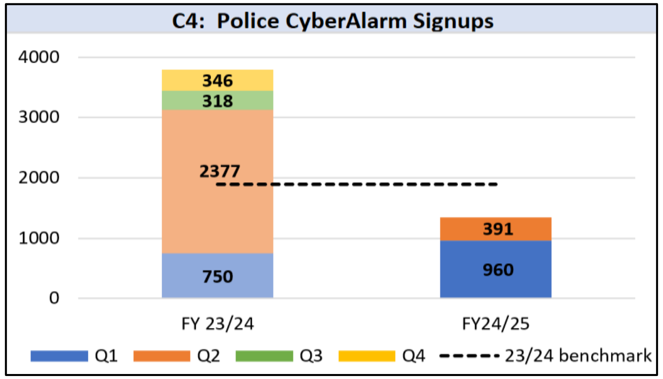
Performance Measure 4: We will ensure ROCUs and Forces are regularly using Police CyberAlarm to help support member organisations when issues are identified and use the data to inform and drive PROTECT, PREVENT and PURSUE activity. PROTECT Officers will promote Police CyberAlarm to all SME organisations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

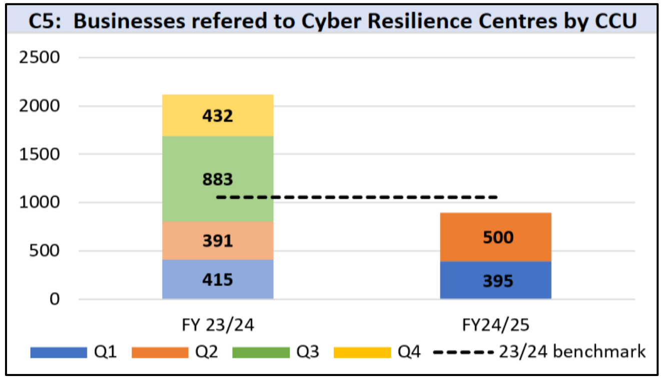
C3 NFIB, TICAT and the NPCC have worked together to produce an operating procedure for the dissemination of three differing types of Protect notifications - Urgent Protect, Protect and Retrospective Protect. These notifications will be sent out by NFIB (unless urgent then directly from source) to the regional Protect teams, and this procedure is due to be rolled out in November 2024.

C5 The recording of these returns has been subject to work on standardising the returns by regions and forces, resulting in the drop from Q3 23/24. Referrals rose to 500 in Q2, an increase of 28% (+109). When divided, Force Cyber Crime Unit referrals increased by 26% (+159) when compared to the same period in 23/24, while the number of Regional referrals decreased by 34% (-70).



C4: Police CyberAlarm Signups

C4 In Q2 391 Small to Medium-sized enterprises (SMEs) signed up to Police CyberAlarm. This is in line with the 23/24 monthly average of 332, but a decrease of 59% (-569) on Q1. This could potentially be due to seasonal adjustments over the summer holiday period meaning that less engagements were held.



C5: Businesses refered to Cyber Resilience Centres by CCU

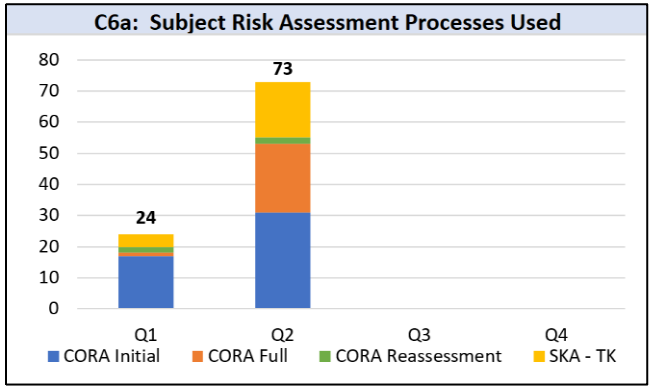
Cyber

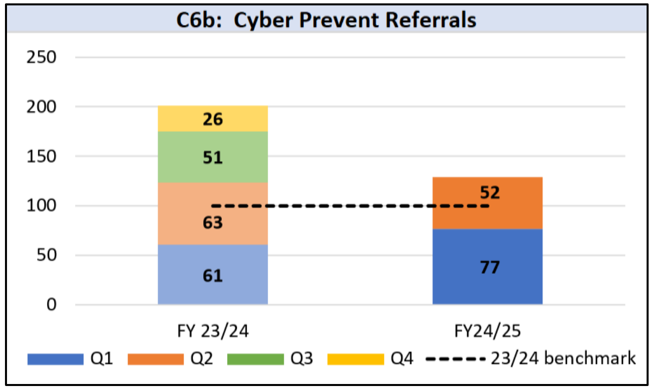
Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

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: Subject Risk Assessment Processes Used


C6b: Cyber Prevent Referrals

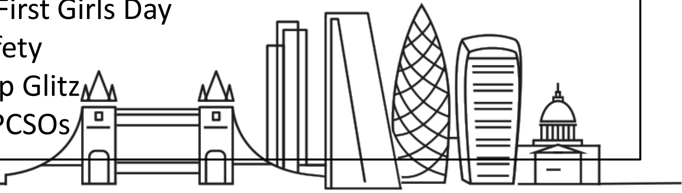
C6a Cyber Operations Rapid Assessments (CORA) consolidate threat, vulnerability, and impact data to equip decision makers with actionable intelligence for securing their cyber infrastructure. The number of risk assessments using this process increased from Q1 to Q2 from 20 to 55, an increase of 175% (+35). Proportionally however, the volume of CORA assessments fell from 83% to 75% in Q2.

C1b A total of 52 Cyber Prevent referrals were received in Q2, down 17% (-11) from Q2 the previous year. However, this was a slight improvement on the 23/24 quarterly average of 50 referrals, and the measure appears on track to improve upon last year's total.

C7 At the end of Q2 there were 103 registered Cyber & Digital Specials and Volunteers registered across 28 forces and regions. Hampshire and TARIAN hold the largest numbers at 14 and 13 respectively. 20 CDSVs logged activity in Q2 which was lower than usual over the summer holiday period.

Some activities logged include:

- Research project into strengthening of cyber security practices amongst private sector organisations that are legally required to store and process sensitive information.
- Dark Net Market monitoring and intelligence generation
- Cyber Protect presentations to various community groups
- Cyber Choices presentation to schools
- Development of interactive Protect activities using CrowPi, AI robot and VR headsets
- Delivered 'Emerging Threats of AI' presentation at NHS staff conference.
- QR Code project - develop educational resources to raise awareness of Quishing.
- Delivered Police Cyber Escape Room
- Created and delivered a presentation on computers and the Law and created an app activity for the students to try at CyberFirst Girls Day
- Delivered School presentation on AI safety
- Completion of evidential package for Op Glitz
- Delivered cyber awareness training to PCSOs

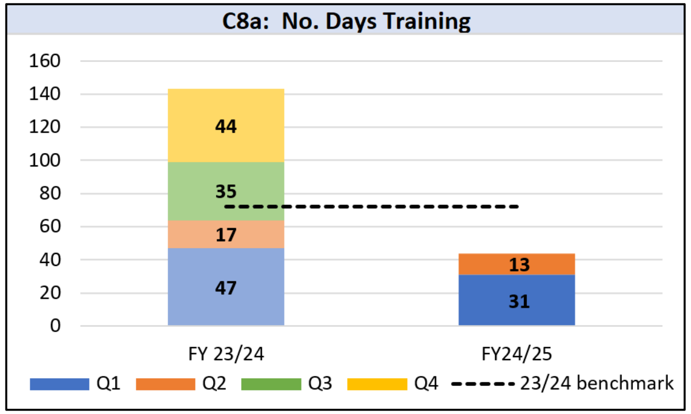


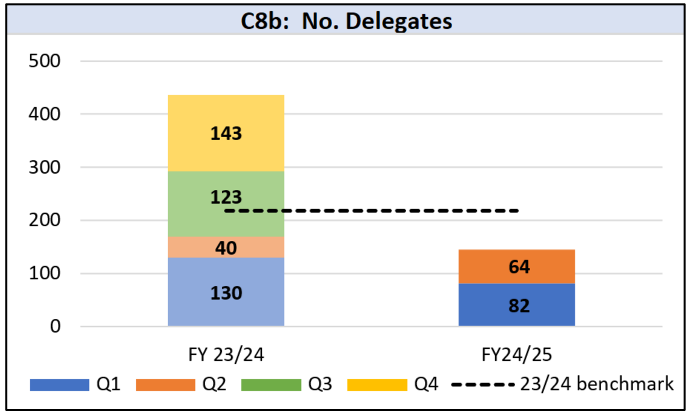
Cyber

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





C8a During Q2 13 days of training were delivered to 64 delegates. The number of courses were down on Q2 23/24 by 23% (-4), and the quarterly average by 64%. However, there is often a seasonal dip in the second quarter and performance is expected to improve in the second half of the year.

C8b The number of delegates followed a similar seasonal pattern with the number for Q2 below the quarterly average for 23/24 by 41% (-45). However, in this case the number of delegates increased from Q2 23/24 to 64, a rise of 60% (+24).

Courses included Neurodiversity and the Police Manager, Cybercrime Foundation Course, Cybercrime Investigation Course and Cybercrime Line Managers Course.

The use of AccessPlanit (the same platform as ECCA) is to go live by the end of October 2024. This will enable all regions and forces to book their own courses, whilst enabling the NPCC to understand the capability of the network.

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. During Q2 24/25 1,947 labs were completed.