National Lead Force
National Delivery Plan Performance Report

FQ2: July – September 2025

Performance Assessment

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

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

Performance Assessment

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

Executive Summary

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

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

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

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

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

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

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

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

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

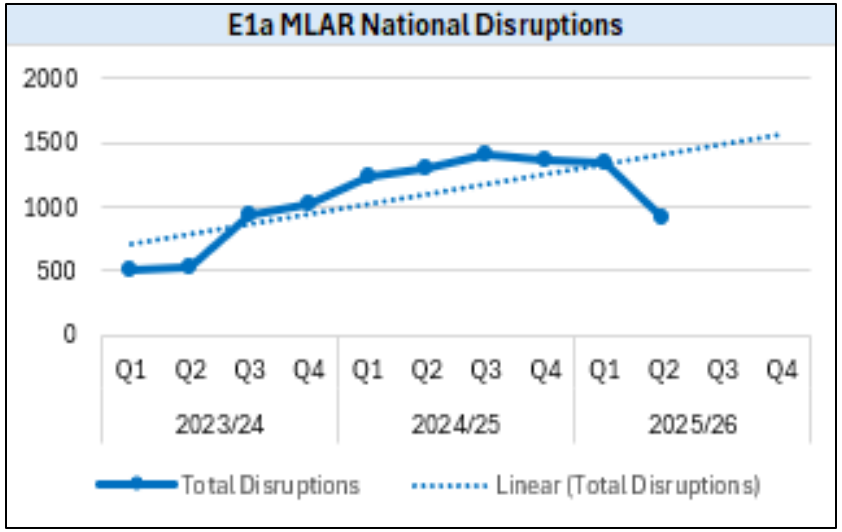
As well as focussed events in Q3 based on seasonal crime trends the delivery of the Fraud and Cyber Crime Reporting and Analysis System will further increase COLPs work to protect people from the threat of fraud, economic and cyber crime.

Money Laundering and Asset Recovery

Improve Outcomes for Victims

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

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



Analysis

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

In Q2, there were a total of 906 disruptions.

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

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

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

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

Home Office Target Not met

Response

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

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

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

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

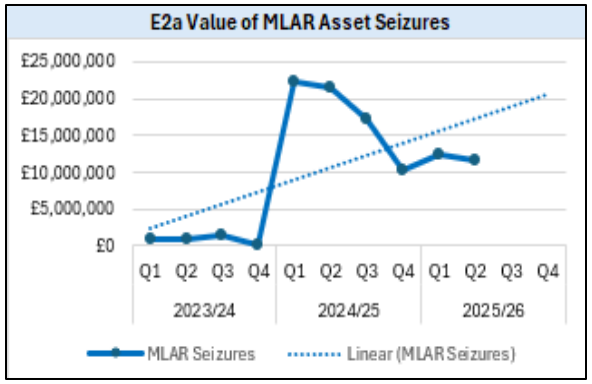
We are expecting to see a rise in disruption activity in Q3 and Q4 as planned operations take place.

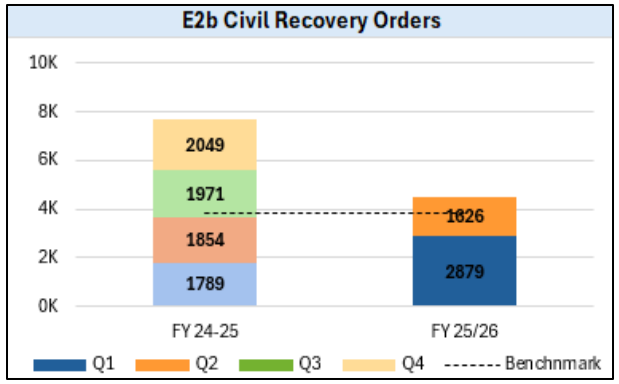
Money Laundering and Asset Recovery

Proactively Pursue Offenders

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

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





Analysis

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

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

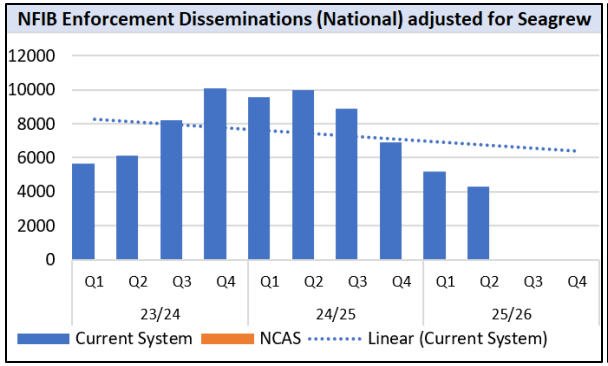
E3 For Q2, there has been £81,751 in cryptocurrency seizures, this is 45% decrease (-£25,317) in comparison to the previous quarter and a 95% decrease in comparison to the same quarter for the previous year (Q2 24/25). The benchmarks for 24/25 is higher due to the significant seizures in Q1, Q2 remains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

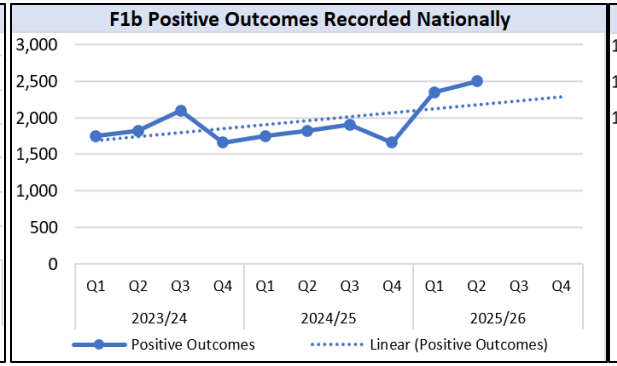
Fraud

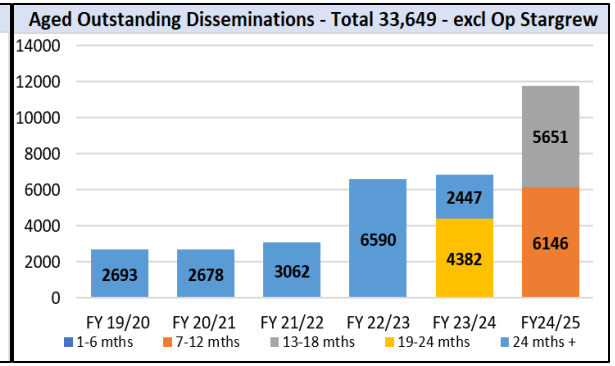
Improve Outcomes for Victims

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

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







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

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

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

Response

NFIB

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

Outcomes

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

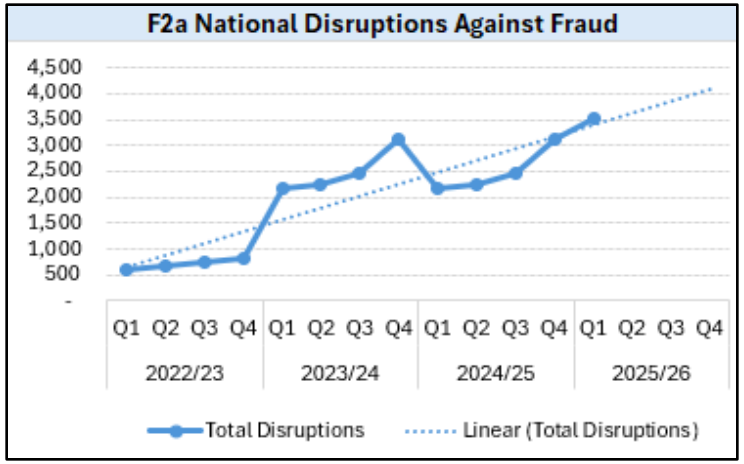
Q1 reflected strong monthly returns from many forces, in combination with large returns from two forces. These totalled more than 350 outcomes from each force in one month. It is these large one-off yields from forces that can push national annual positive outcomes from circa 6k to 8k per annum and even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

Fraud

Proactively Pursue Offenders

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

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



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

For fraud related disruptions there were:

- 33 major disruptions - 43% increase (+10) in comparison to Q1 24/25.

Offender disruption accounted for 65% (26) of major disruptions, this includes actives such as arrests, convictions, warrants/searches.

- 173 moderate disruptions - 12% increase (+18) in comparison to Q1 24/25.

Offender disruption was also the highest activity for moderate disruptions at 42% (115).

- 3,309 minor disruptions - 66% increase (+1,316) in comparison to Q1 24/25.

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

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

Home Office Target Exceeded

Response

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

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

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

Fraud

Proactively Pursue Offenders

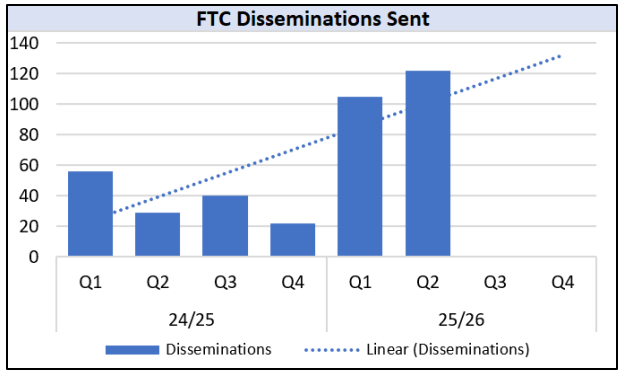
Performance Measure 3: We will lead the National Fraud Squad to PURSUE identified high harm offenders through joint, centrally co-ordinated national operations and to participate in NECC led fraud intensifications throughout the year.
Performance Measure 4: We will support and assist the national development and implementation of the Fraud Targeting Cell by contributing resource and supporting the delivery of systems and processes. We will increase intelligence packages into the system leading to increased proactive operations

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

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

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

Home Office Target Met



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

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

Response

Intensifications

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

FTC

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

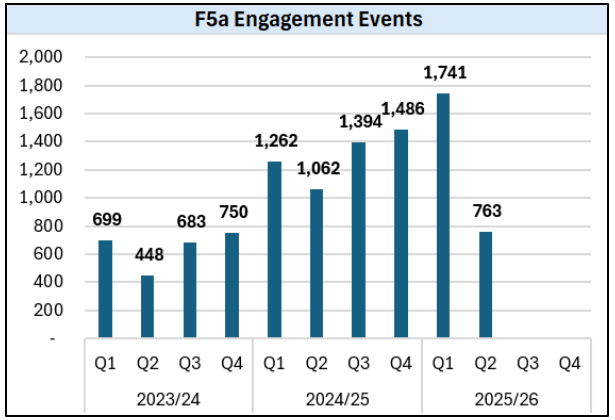
New SIM Farm Approach - Joint working between FTC, NCA FIT and CoLP has resulted in the attribution of six UK based handsets believed to be orchestrating bulk scam messaging campaigns impacting the UK. Executive action is planned for November.

Fraud

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

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

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



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

F5b&c The fraud protect surveys continue to be adopted by the national Fraud Protect Network during their presentations, events and interactions with citizens and businesses across the country. In FQ2

98% were very satisfied and satisfied with the event/engagement (no change from Q1)

99% were likely to change their behaviour or already undertake that behaviour (1% increase from Q1).

Home Office Target Met

In Response

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

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

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

This more directed approach in Q3 will focus on

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

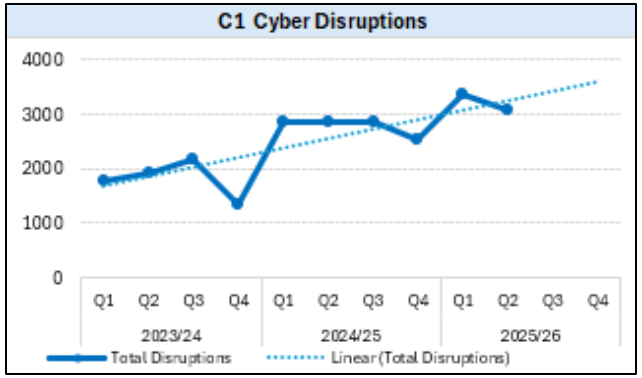
The network will be partnering with Barclays during November, collaborating on delivering a consistent national protect message with protect officers and Barclays staff. This will also utilise Barclays 'scam vans' in 40 retail locations throughout the UK delivering consistent protect advice to the public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

Cyber

Improve Outcomes for Victims

Performance Measure 1: We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance from forces to record disseminations from the NFIB appropriately and that subsequent outcomes are reported back to NFIB correctly.
Performance Measure 2: We will increase intelligence led proactive operations and self-development operations regarding Computer Misuse Act offending, ensuring the relevant deconfliction safeguards are followed.

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



C1. In Q2, there were a total of 3,082 disruptions.
- 1 major disruptions - 75% decrease (-3) in comparison to Q1 25/26
- 66 moderate disruptions - 1% decrease (-1) in comparison to Q1 25/26
- 3,015 minor disruptions - 9% decrease (-288) in comparison to Q1 25/26.

The top 2 disruption types are specialist advice at 79% (2,436) and safeguarding at 11% (330).
In comparison to the previous quarter (Q1), Cyber disruptions are reporting a 9% decrease (-292). In comparison to the same quarter for the previous year (Q2 24/25), there has been an 8% increase (+221).
The benchmark from 24/25 is 11,085, which translates to 2,771 disruptions per quarter. For the FYTD Q2, disruptions are 16% (+914) above the benchmark.

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

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

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

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

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

Cyber

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

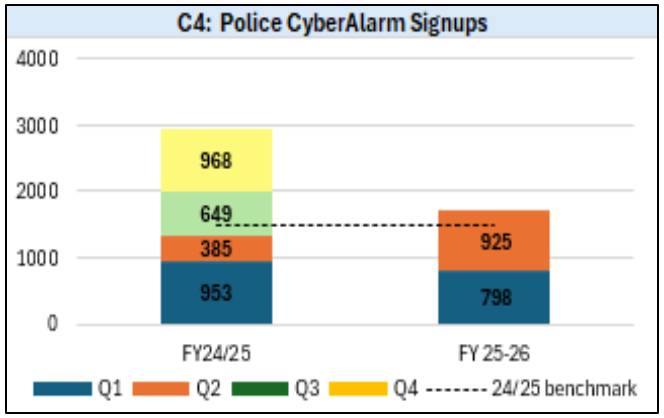
Performance Measure 3: We will develop the current PROTECT notification processes to ensure a consistent approach to both the direct PROTECT officer taskings and the notifications delivered at scale.

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

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

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

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



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

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

Response

Protect Notifications

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

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

PCA

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

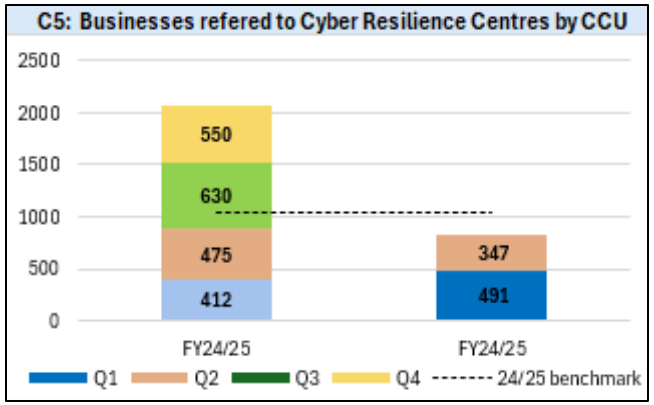
However, in August 2025, PCA changed the registration process to make it quicker and easier with automated approvals and fewer registrations details required, which is likely to increase the number of sign-ups. Furthermore, PCA have commenced the use of a marketing company, with the aim to increase growth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

Cyber

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

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

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



C5

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

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

Response

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

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

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

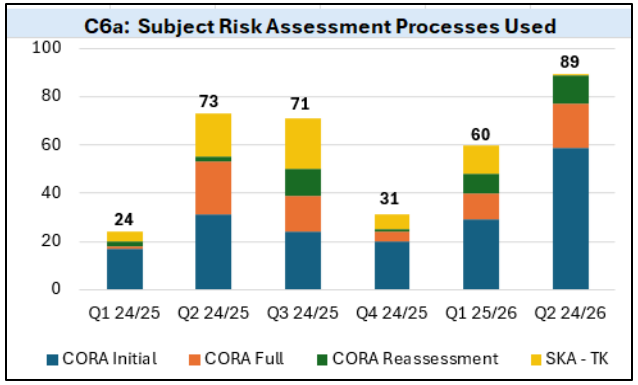
The new CRC Strategy and Delivery Plan will focus on membership growth, Cyber Path delivery and Cyber Essentials.

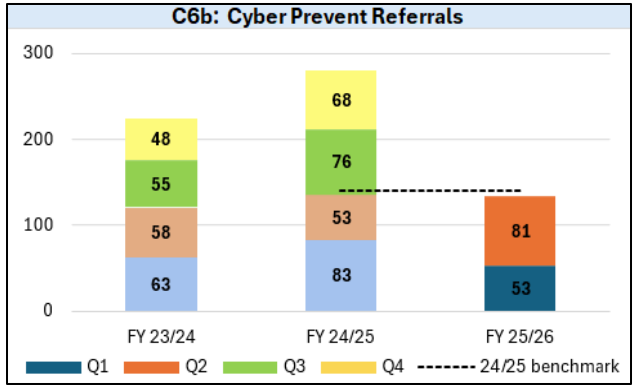
Cyber

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

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

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





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

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

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

Response

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

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

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

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

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

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

Cyber

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

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

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

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

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

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

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

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

Response

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

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

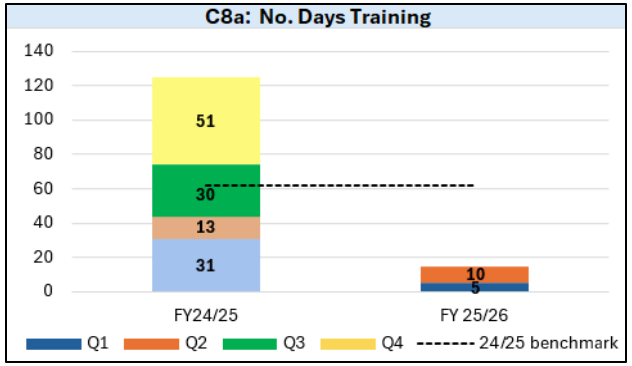
CDSV will be rebranded to become the Specialist Crime Volunteer Network (SCVN) and will encompass not only cyber but support to the wider economic crime portfolio. This wider support and growth will be a key priority for the new team when they start.

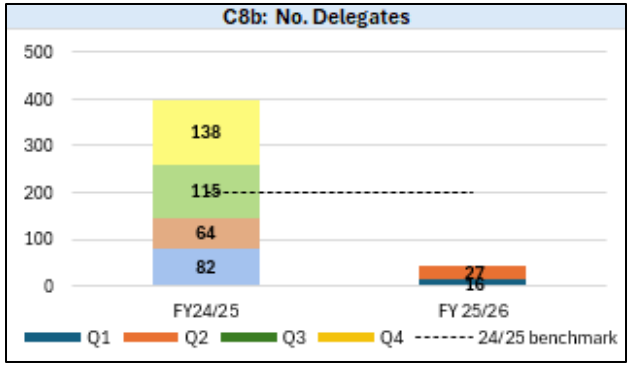
Cyber

Improve Outcomes for Victims

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

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





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

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

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

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

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

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

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

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