National Policing Strategy for Fraud, Economic and Cyber Crime 2023-2028

Closure Report

November 2026







Contents

Foreword page 1

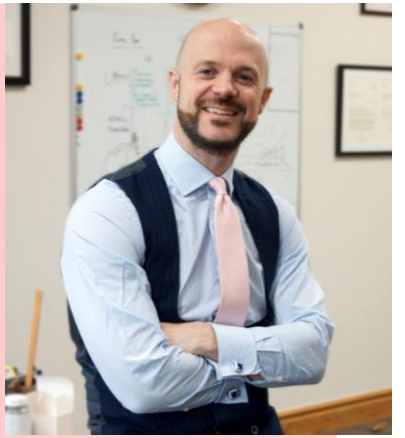
Executive Summary page 2

Fraud page 11

Money Laundering and Asset Recovery page 19

Cyber page 27

Foreword



Fraud, economic crime and cyber crime continue to cause immense harm to individuals, businesses and communities across the UK. Behind every report is someone who has lost money, confidence, security or trust. For many victims, the impact extends far beyond the financial loss, affecting their wellbeing, livelihoods and sense of safety. It is those people who have remained at the heart of this strategy from the very beginning.

The National Policing Strategy for Fraud, Economic and Cyber Crime was established to strengthen the policing response to these increasingly complex threats. As this report demonstrates, we have delivered significant and lasting change. Through strong partnerships, sustained investment and the dedication of colleagues across policing and beyond, we have achieved 95% of the strategy's objectives and created capabilities that will continue to protect the public well into the future.

Among the most significant achievements has been the implementation of Report Fraud, providing a more effective service for those reporting fraud and improving the intelligence available to policing. We have established the National Fraud Squad and Fraud Targeting Cell, strengthened victim care services, enhanced our economic crime capabilities and invested in the specialist cyber expertise needed to tackle emerging threats. Collectively, these developments have transformed our ability to identify, disrupt and pursue offenders while providing better support for those affected by crime.

I am particularly proud of the people behind these achievements. Change on this scale is never straightforward. It has required vision, resilience and an unwavering commitment to public service from colleagues across forces, regional organised crime units, government departments and partner organisations. Their determination to improve outcomes for victims and stay ahead of increasingly sophisticated criminals has been exceptional.

This report marks the successful conclusion of one strategy, but not the end of our ambition. Criminals will continue to evolve, exploiting new technologies and operating across borders. Our response must continue to adapt accordingly. The foundations established through this programme mean policing is now better equipped than ever before to prevent harm, support victims and bring offenders to justice.
As we look ahead to the next phase of this work, we do so from a position of strength. The capabilities, partnerships and expertise developed through this strategy provide a strong platform for the future. Most importantly, they help ensure that more victims receive the support they need and that more offenders are held to account.

That must remain our shared purpose.

Pete O'Doherty, Commissioner

Executive Summary

The **National Policing Strategy for Fraud, Economic and Cyber Crime 2023-2028** was launched in November 2023, combining Home Office and NCA strategies and action plans into one policing strategy. Home Office investment into fraud, cyber and money laundering via the Fraud Reform, AMLAR and Cyber programmes delivered growth and new capabilities within policing that have changed the policing response.

The 2023 Strategy was the first combined fraud, economic crime and cyber crime strategy, and enabled the successful delivery of strengthened victim services, increased proactive disruption of offenders, enhanced national protect activity, and improved policing capability, governance and performance. Of the objectives set out within the strategy, **95% have been delivered**, providing a strong foundation for future development and leading to the decision to conclude the strategy two years ahead of schedule.

A major achievement has been the successful implementation of **Report Fraud**, replacing legacy Action Fraud and National Fraud Intelligence Bureau systems with a modern, intelligence-led reporting and analysis service. The platform has improved accessibility, victim experience and analytical capability, while significantly reducing processing times and improving the quality of information available to law enforcement.

Across the **Fraud** threat area, policing has delivered all strategic objectives, including the establishment of the **National Fraud Squad**, **Fraud Targeting Cell**, **National Protect Network**, and the expansion of the **National Economic and Cybercrime Victim Care Unit**. These capabilities have enabled a shift towards proactive, intelligence-led enforcement, resulting in thousands of disruptions, significant asset seizures and coordinated national operations targeting high-harm offenders and organised fraud networks.

The **Anti-Money Laundering and Asset Recovery (AMLAR) Programme** has strengthened the policing response to money laundering through investment in specialist financial investigators, intelligence professionals and dedicated national capabilities. New regional and national teams have increased asset denial activity, enhanced intelligence development and improved the identification and disruption of money laundering networks. Specialist crypto asset recovery capabilities, supported by legislative reform and enhanced technology, have further improved law enforcement's ability to identify, seize and recover criminal assets in an increasingly digital landscape.

The **Cyber Portfolio** has achieved all strategic deliverables and established a more coordinated national response to cyber crime. Through the Nationally Led, Regionally Managed, Locally Delivered model and enhanced intelligence capabilities and initiatives such as **Project Capstone**, policing has increased its ability to identify and disrupt cyber offenders, resulting in the seizure of over **£40 million in criminal assets**. Investment in cyber resilience has also delivered significant benefits, with the **Cyber Resilience Centre Network** supporting more than **31,000 organisations**, while **Police CyberAlarm** has identified over **one billion suspicious cyber events**, helping businesses and communities reduce their vulnerability to attack.

This strategy has also delivered substantial progress across its cross-cutting objectives. Collaborative partnerships with government, industry, academia and international law enforcement agencies have strengthened operational capability and innovation. Investment in the workforce through programmes such as the Police Now Economic Crime Pathway, the Economic and Cyber Crime Academy, specialist volunteering and professional development initiatives has helped build a more skilled, diverse and sustainable workforce. Enhanced governance arrangements, national performance frameworks and investment in data and technology have improved transparency, accountability and the ability to measure impact across policing.

While fraud, economic crime and cyber crime continue to evolve and present significant challenges, the strategy has successfully delivered a step change in capability, coordination and performance. Policing is now better equipped to protect the public, support victims, pursue offenders and disrupt criminal networks. The infrastructure, partnerships and capabilities established through this strategy provide a strong platform for the next phase of development, with a new national strategy due to launch later in 2026 aligned to updated government priorities.

Improved Outcomes for Victims

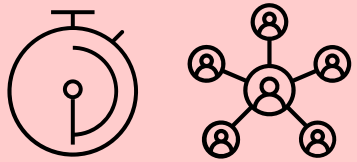
PILLAR ONE

Improving outcomes for victims was a central pillar of the strategy and reflected widespread recognition that the policing response to fraud and cyber crime had failed to keep pace with victim demand and harm.

The most significant intervention during the strategy period was the replacement of the legacy Action Fraud and National Fraud Intelligence Bureau systems with the new Report Fraud service. This transformation has improved the accessibility of reporting, enhanced the quality and timeliness of intelligence provided to policing partners, and laid the groundwork for a more transparent and responsive victim experience.



Improved the accessibility of reporting



More timely, better quality intelligence sharing with partners



More transparent and responsive victim care

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

Report Fraud

Report Fraud

The Next Generation Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) Programme, was established in 2020 to create a unified, modern system for reporting and analysing fraud and cybercrime. Led by the Home Office with procurement delegated to the City of London Police, the programme combined multiple services into a single cohesive platform. It has been primarily government-funded, with additional financial support from the City of London Corporation. The initiative was designed to integrate fraud reporting into a broader law enforcement ecosystem, enabling better data sharing with partners and improving collaboration across agencies to strengthen investigations and response capabilities.

The Report Fraud service launched in January 2026, marking the successful conclusion of the (FCCRAS) programme and the transition to a new target operating model for fraud and cybercrime. The service represents a significant step forward in the national response to fraud and cybercrime, with a clear commitment to ensuring that every report counts.



At its core, Report Fraud delivers an end-to-end service built on advanced technology and data analytics. It enhances reporting through an accessible, trauma-informed, multilingual platform that allows victims to submit detailed reports, including supporting evidence, via multiple channels.

The system processes around 35,000 reports per month, alongside similar volumes from industry partners such as Cifas. It incorporates automation, interoperability, and data-linking capabilities to improve efficiency and insight generation. These features support key strategic objectives such as improving victim experience, enhancing criminal justice outcomes, preventing crime, and strengthening understanding of serious and organised threats—while aligning with national strategies like the UK's Cyber Strategy and Fraud Strategy.

The service also includes advanced analysis and crime management functions powered by the NCAS Foundry platform, which links and prioritises cases based on risk, harm, and solvability.

Reports are assessed, grouped, and developed into actionable intelligence before being disseminated to law enforcement bodies or escalated to specialist agencies where necessary. Early performance indicators show significant improvements, including faster case processing times, higher satisfaction rates among victims, and increased responsiveness. Since launch, the system has helped recover £1.8 million for victims. As a complex programme involving multiple workstreams and significant investment, Report Fraud is designed for continuous improvement and growing collaboration, with an emphasis on maintaining a unified approach to maximise its long-term value.

NCAS enhancements to date include Victim List enhancement, Victim Comms Protect Advice updates, improvements made to Outcome Codes and Data, and Enhanced Search and Filter Options.

Key Highlights of the Report Fraud Service

- Overall reporting has grown, and with the new capability to ingest reports presented to CIFAS now coming into Report Fraud as Crime Reports overall, we see consistently just under 80,000 reports of crime or suspicious activity being received monthly.
- Support provided by Victim Services continues to have a strong positive impact on victims, with 88% (589 of 672) reporting they were either satisfied (16%) or very satisfied (72%) with the services received throughout 26/27 Q2. Victim services have supported over 150,000 victims since Report Fraud launched.
- Between April-November 2025, average call wait time for Action Fraud was 13m 52s with an abandonment rate of 18.26%. Between December 2025 to present, the Report Fraud average call wait time was 1m 8s with an abandonment rate of 8.8%. Action Fraud answered, on average, 28k calls a month, with Report Fraud answering an average of 33k calls a month.
- Disseminated reports have increased by 1,579 (62.7%) since go-live, with an average increase of approximately 395 reports (13.5%) each reporting period, with the average time to disseminate a report reducing from 37 days to 5 days. In addition, Report Fraud has already supported various international operations with intelligence disseminations.
- Report Fraud to date has referred 16,000 disruption notices to industry with confirmed take-down actions for 8,300 criminal entities across email accounts, websites, telephone numbers and social media accounts.

Proactively Pursue Offenders

PILLAR TWO

There has been a clear systemic shift in policing away from reactive investigations toward proactive disruption of organised crime groups operating across fraud, economic, and cybercrime. Rather than focusing primarily on responding to individual cases, law enforcement is increasingly prioritising early intervention, targeting criminal networks, and disrupting the tools, infrastructure, and enablers that underpin large-scale offending.

This approach is exemplified by the creation of the National Fraud Squad (NFS) in 2023, jointly led by the National Economic Crime Centre (NECC) and the City of London Police (CoLP). The NFS has brought together regional and national capabilities, including Proactive Economic Crime Teams, to operate both locally and as a coordinated national network. Its model enables intelligence-led activity to identify and target high-harm offenders, while also addressing the wider systems and technologies that facilitate fraud, both within the UK and internationally.

National intensification tactics have played a key role in delivering this proactive strategy, proving effective over the past three years. These coordinated efforts have led to increased disruption of organised crime groups, greater asset seizures, and enhanced collaboration across policing and law enforcement agencies. This shift has strengthened the overall response to fraud and economic crime, moving the system toward a more preventative, intelligence-driven model.



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

PILLAR THREE

The past three years has seen huge steps forward in a more co-ordinated national Protect response to fraud and cyber crime.

The National Protect Network was funded by the Fraud Reform Programme from 2023, enabling dedicated Fraud Protect Co-ordinators in each region and new national co-ordination functionality within CoLP. This network has now merged with the National Cyber Protect Network to allow for a more joined-up approach, co-ordinating rapidly changing protect advice for victims, and launching a national protect calendar with assets and advice produced centrally to feed into it.

The National Protect Strategy was launched in 2026 and seeks to deliver a co-ordinated approach to National Protect under three core pillars.

The Protect Network is the delivery and preventative arm of policing for fraud and cyber crime. It works with communities, businesses and partner organisations to raise awareness, reduce vulnerability, improve cyber resilience, and prevent people from becoming victims through education, engagement and intelligence-led protect activity.

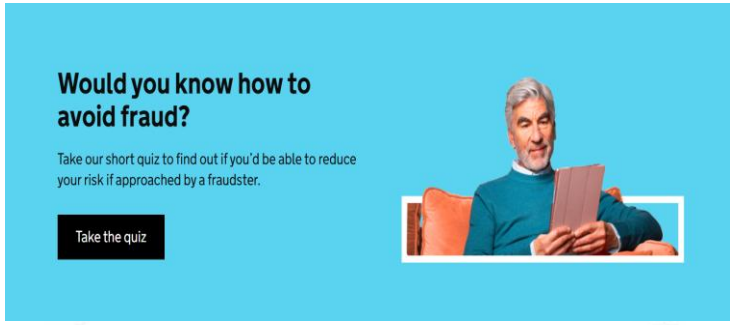




Protect People and Businesses from the Threat of Fraud, Economic and Cyber Crime

PILLAR THREE





Stop! Think Fraud

The **Stop! Think Fraud** campaign, launched in February 2024 by the Home Office, in partnership with the National Cyber Security Centre (NCSC), City of London Police, National Crime Agency (NCA), and other organisations, aims to empower the public to protect themselves against scams and fraudsters.

The campaign provides clear, consistent advice on:

- reducing the risk of becoming a victim
- information on reporting fraud via Report Fraud
- recovering from fraud in both practical, emotional support and recovering financial losses.

CoLP have worked with all the organisations mentioned above to produce a single Protect calendar bringing campaigns together based on a Report Fraud evidence providing more campaign consistency.

Collaborative Working

Collaboration remains central to strengthening the national response to fraud, economic crime and cyber crime. Over the 3 past years, significant progress has been achieved through partnerships across law enforcement, government, industry and international stakeholders, enhancing operational effectiveness, capability development and prevention activity.

Internationally, the City of London Police has worked closely with the National Economic Crime Centre (NECC) to implement recommendations arising from **Operation Winterproof**, strengthening the collective response to emerging global fraud threats. This has included the delivery of bespoke training programmes to investigators in high-risk jurisdictions, enhancing investigative capabilities and supporting more effective cross-border cooperation. In early 2026, the Economic Crime Academy (ECCA) delivered specialist training to officers in Nigeria and South East Asia, with further phases planned to deepen relationships and build international capability.

Chief Officer engagement and overseas visits and visitors to the UK have also strengthened strategic partnerships with counterparts in Nigeria, Ghana and India, helping to influence and promote greater cross-border operational collaboration against transnational criminal networks.

Strong partnerships with the private sector continue to underpin innovation across the economic crime landscape. Collaborative working through industry-funded units has continued, while ongoing engagement with partners has supported the continuous improvement roadmap for the **Report Fraud** service, ensuring technology and processes evolve to meet emerging threats and user needs. Protect activity has also been strengthened through the expansion of brand partnerships, enabling trusted organisations to amplify prevention messaging, increase public reach and help protect individuals and businesses from fraud at scale.

The Cyber Resilience Centre (CRC) Network provides a further example of successful collaboration in action. Bringing together policing, government, academia and industry, the network now supports more than 31,000 businesses across England and Wales with trusted cyber resilience advice and services.

Through its growing National Ambassador Programme and extensive regional partnerships, the CRC Network combines policing's crime prevention expertise with private sector knowledge, funding and innovation, delivering tangible improvements in cyber resilience and extending support to communities and businesses nationwide. Together, these collaborative initiatives demonstrate the value of partnership working in driving innovation, strengthening capability and improving outcomes across the economic crime and cyber landscape.



Cross Cutting Objectives

Workforce Strategy

The Workforce Strategy has delivered significant progress in attracting, recruiting, supporting and retaining a skilled and diverse workforce for economic crime policing. A key achievement has been the development and expansion of the Police Now Economic Crime Pathway, led by the City of London Police. Following the successful delivery of two cohorts, a third will commence in 2027, providing an accelerated route into economic crime investigation and supporting future leadership development. Supported by training through the Economic Crime Academy (ECCA), the programme has gained national recognition, with additional forces now developing their own pathways. It has also contributed to workforce diversity objectives, attracting individuals who had not previously considered a policing career and increasing representation of women and people from ethnic minority backgrounds.

Further progress has been made through initiatives designed to strengthen talent pipelines, professional development and knowledge sharing.

The Financial Investigator Intern Programme has expanded from a successful pilot to a national scheme across multiple forces and ROCUs, creating a valuable entry route into specialist economic crime roles.

The **Cyber Digital Specialist Volunteer (CDSV) Network**, rebranded in 2026 as the **Specialist Crime Volunteer Network (SCVN)**, provides policing with access to specialist skills, industry expertise and additional capacity across cyber, economic crime and serious organised crime.

Volunteers support Protect and Prevent activity by working with Cyber Resilience Centres, Cyber Protect and Fraud Protect teams to engage businesses and communities, deliver cyber awareness initiatives and run cyber security exercises. They also contribute specialist expertise in areas such as cyber security, artificial intelligence, dark web monitoring, intelligence development and open-source intelligence (OSINT), while supporting investigations, victim care and cyber offender interventions. The network is increasingly embedded across policing, with volunteers supporting local, regional and national tasking. During 2025/26, **146 volunteers** were active across the network, delivering **125 volunteering activities** and contributing **478 hours of support**.

Funding has enabled a range of innovative projects, including volunteer-developed Protect tools, OSINT capabilities, technology-enabled abuse prevention initiatives and cloud-based training environments. Recognising the value of this capability, the Cyber Policy Unit doubled programme funding during 2025/26, supporting the recruitment of dedicated leadership and coordination roles from 2026/27.

The network has also been incorporated into the **Science and Technology in Policing Strategy** and is recognised within the development of future government cyber and fraud policy, reflecting its growing role in addressing specialist skills shortages across policing.

Supporting this capability is the national **Assemble** platform, which enables specialist volunteer skills to be accessed across forces, ROCUs and the NCA, ensuring expertise can be deployed where it is needed most. This scalable and cost-effective model strengthens workforce resilience, increases operational capability and provides access to skills that would otherwise be difficult to source within policing.

The Economic Crime Academy (ECCA) has continued to strengthen workforce capability through an expanded curriculum, delivering new and specialist training programmes aligned to College of Policing standards and designed to meet emerging operational needs. In partnership with the College of Policing, the ECCA developed the first *Fraud, Economic and Cyber Crime for the Frontline* programme, which launched in June 2026 to equip first responders and contact staff with the knowledge and skills required to identify and respond effectively to cyber and economic crime. The Academy is also proactively addressing capability gaps identified through HMICFRS PEEL inspections, designing and delivering targeted training interventions to support forces in meeting the required standards and improving the policing response to fraud, economic and cyber crime.

SCVN
SPECIALIST CRIME VOLUNTEER NETWORK
Operated by City of London Police

CDSV
CYBER AND DIGITAL SPECIALS AND VOLUNTEERS



Cross Cutting Objectives

Governance and Performance

Following the launch of the Strategy in November 2023, a comprehensive performance framework was introduced to monitor progress against the objectives set out in the Strategic Plan.

This performance pack represented the first national approach to measuring policing activity across fraud, economic crime and cyber crime. It brought together national data from APMIS, Action Fraud and JARD to provide consistent performance measures and improved oversight of delivery across the network.

The introduction of national performance monitoring has highlighted a number of challenges, including inconsistent definitions of disruption activity, duplicate reporting and knowledge gaps in data recording practices. Identifying these issues through a national governance framework has enabled the development of coordinated improvement plans, which are now being implemented across policing to strengthen data quality and consistency.

The launch of Report Fraud in January 2026 provides the policing network with access to a significantly enhanced analytics platform, enabling more accurate and timely analysis of fraud and cyber crime reports submitted nationally.

This represents a transformative step forward in the measurement and understanding of reactive policing activity across fraud and cyber crime. The platform will deliver improved insight into reporting trends, demand, victim profiles, investigative outcomes and operational performance, supporting more informed decision-making at both local and national levels.

Data and Technology

Significant progress has been made over the past three years in enhancing the use of data and technology to tackle fraud and cybercrime.

The launch of **Report Fraud** marked a major milestone in the successful delivery of a five-year transformation programme. Through the implementation of cutting-edge technology, the programme has strengthened the use of fraud and cybercrime reports to better identify, target and disrupt criminal activity. It also provides a foundation for the continuous development of data-sharing capabilities and operational effectiveness.

The City of London Police, working in partnership with the Police Digital Service and the Home Office, is leading the transformational **Asset Recovery IT (ARIT)** programme to replace the Joint Asset Recovery Database (JARD). Scheduled for delivery within the next two years, ARIT will provide enhanced functionality and improve the recording, management and tracking of seized and restrained assets across the UK.

Improving data sharing across the economic crime and cyber landscape remains a key priority and is reflected within the forthcoming **Economic Crime Plan 26-29**. This will set out the next steps required to strengthen information sharing, improve operational efficiency and enable a more coordinated response to economic crime.

FRAUD

We achieved 100% of the deliverables outlined in the strategy for fraud.

Policing delivered:

- Report Fraud
- National Fraud Squad
- Fraud Targeting Cell
- National Protect Network
- Expansion of National Economic Crime Victim Care Unit

The Fraud Strategy 2023 – 2026 laid out the government objective to reduce fraud by 10%. The first fraud strategy of its kind, it delivered funding through the Fraud Reform Programme, to change the system response to fraud through investment in law enforcement and tracking of objectives under three core pillars:-



The National Policing Strategy took the objectives from this strategy and translated it into 11 work package deliverables and 15 performance objectives for policing.

Pursue fraudsters
Pillar One

Block fraud
Pillar Two

Empower people
Pillar Three

By the end of financial year 25/26, all Fraud Strategy 2023 – 26 deliverables and objectives were completed.
The new Home Office Fraud Strategy 2026 – 29 launched in March 2026, signalling a new direction which will be reflected in a new National Policing Strategy.

FRAUD

Deliverables

Improve outcomes for victims	Proactively pursue offenders	Protect people and businesses
We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages.	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 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.
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	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 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 support forces in their ambition to have sufficient resources in place to effectively deal with the threat of fraud in accordance with the Strategic Policing Requirement and the NLF Force Improvement Plan.	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 task overt and covert intelligence assets to fill national intelligence requirements set by the FTC. We will increase intelligence packages into the system leading to increased proactive operations.	We will deliver enhanced victim care and support to victims of fraud and cyber crime, to reduce harm of offending and prevent re-victimisation.

Improved Outcomes for Victims

The key deliverable under the Fraud Strategy to improve outcomes for victims was the successful implementation of the **Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS)**. As outlined in Section 1, **Report Fraud** was publicly launched in January 2026, marking the culmination of a five-year transformation programme to modernise the way fraud and cyber crime is reported, assessed and utilised across law enforcement. The programme has replaced legacy systems with a modern, technology-enabled service that provides a more efficient and user-focused reporting experience while significantly enhancing the ability of policing and partners to analyse intelligence and identify criminal activity.

Report Fraud has created a single national platform for fraud and cyber crime reporting, enabling better use of victim reports, improved intelligence development and more effective identification of crime trends, vulnerabilities and organised criminal networks. Through enhanced data analytics, automation and information-sharing capabilities, the service supports a more targeted and coordinated law enforcement response, helping to identify opportunities to disrupt offenders and prevent further victimisation. The system has also been designed with future integration and scalability in mind, ensuring it can adapt to evolving threats and emerging technologies.

The **Fraud Strategy 2026-2029** builds on this achievement by focusing on embedding the service across the law enforcement and partner landscape and ensuring the full benefits of the investment are realised. This includes further enhancing analytical capability, improving data sharing with public and private sector partners, strengthening operational outcomes through better intelligence exploitation, and continuously improving the experience for victims. By maximising the value of the information provided through Report Fraud, policing will be better placed to identify high-harm threats, coordinate activity across jurisdictions and deliver a more effective response to fraud and cyber crime.

Coordinated Response

In 2023, a commitment was made to support policing services in achieving sufficient resourcing to respond effectively to the threat of fraud. This aligned with the requirements set out in the Strategic Policing Requirement (SPR) and the National Law Enforcement Fraud (NLF) Improvement Plan.

- Ongoing collaboration with HMICFRS successfully secured the inclusion of fraud within the PEEL inspection framework, marking a critical step in strengthening accountability and performance oversight across all forces.
- Following publication of the Fraud Strategy, the Force National Co-ordinators Office (NCO) continued to provide targeted support to forces in implementing the Force Improvement Plan, ensuring alignment with national expectations.

The inclusion of fraud within PEEL inspections has driven greater organisational focus, capability development, and performance scrutiny across all 43 police forces. The first tranche of PEEL reports incorporating fraud assessments is currently being published, providing valuable insights into force-level strengths and areas for improvement. The NCO continues to play a central role in supporting forces to respond to inspection findings and embed improvements. The Economic and Cyber Crime Academy is delivering targeted training programmes to address identified capability gaps in the policing response to fraud.

NECC
NATIONAL ECONOMIC CRIME CENTRE
A multi-agency unit housed in the NCA

Proactively Pursue Offenders

FRAUD

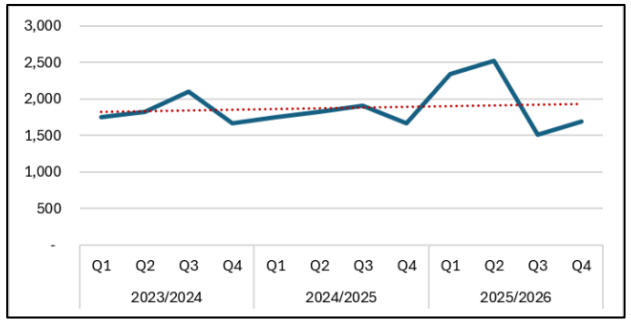
The 2023 Fraud Strategy signalled the delivery and launch of a new National Fraud Squad (NFS). Made up of a network of existing and new teams across law enforcement, specifically the NCA and Policing, the NFS was designed to provide a networked proactive approach to tackling fraud and fraud enablers.

New Proactive Economic Crime Teams (PECT) were delivered in every region in England and Wales – these were entirely new teams with a remit to both deliver national outcomes and SOC disruptions and to also undertake operational activity that supported local intelligence development.

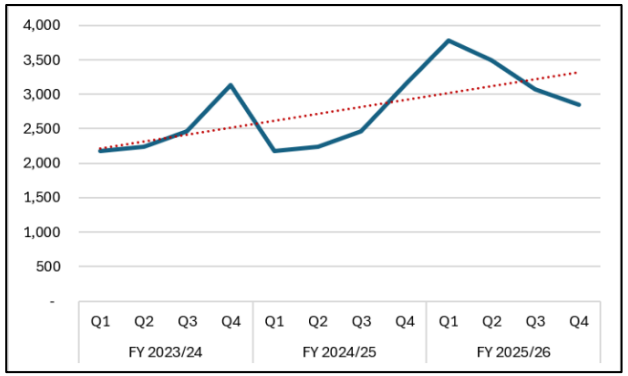
Since 2023, the PECTs have disrupted 2192 incidents, seized £25,991,768 in assets, issued 276 disposals (including charges, cautions, absconders, extradition, prison recall, NFA and deceased), and made a total of 569 arrests since 2024.

In 2025, the London PECT became the last of these teams to join the network – and has already successfully arrested 19 suspects and achieved 34 disruptions against the fraud threat.

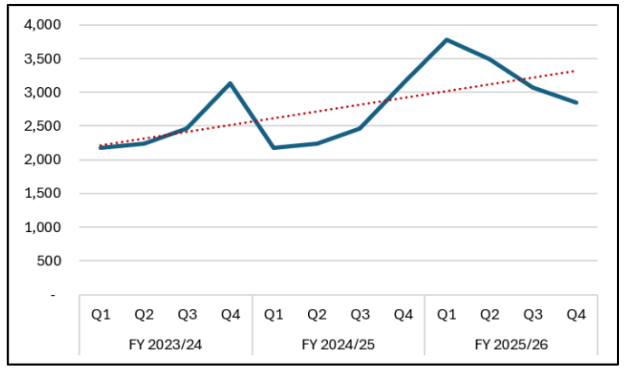
National Positive Outcomes



National Fraud Disruptions



National PECT Disruptions



Fraud Targeting Cell

In 2023, the NECC co-established the Fraud Targeting Cell (FTC) in partnership with the City of London Police. The FTC built upon the capabilities previously provided by the City of London Police Intelligence Development Team, combining those resources with NCA intelligence to create a strengthened national intelligence function.

The FTC receives intelligence and information from a wide range of sources and transforms this material into actionable, proactive intelligence packages for law enforcement partners across the country. By bringing together national intelligence assets and specialist analytical capability, the FTC has enhanced the ability of policing and partner agencies to identify, target and disrupt fraudsters operating at scale.

Since its inception, the FTC has produced and disseminated 561 proactive intelligence packages, providing law enforcement agencies with timely opportunities to pursue offenders, prevent further victimisation and support coordinated enforcement activity. The development of the FTC represents a significant step forward in the national intelligence-led response to fraud, ensuring that intelligence is translated into operational opportunities that deliver tangible outcomes against fraud threats. Therefore, FTC is due to be brought into Report Fraud.

NECC
NATIONAL ECONOMIC CRIME CENTRE
A multi-agency unit housed in the NCA

National Intensifications

Report Fraud | CITY OF LONDON POLICE

FRAUD

Operation Henhouse

A key operational deliverable of the National Fraud Squad (NFS) has been the use of national intensification activity to target suspects and disrupt criminality. Since its inception, the NFS has delivered a series of coordinated national intensification operations focused on a range of fraud threats, including courier fraud, romance fraud and investment fraud.

In addition, the NFS has conducted the annual Operation Henhouse intensification each February, providing funded overtime and enhanced operational activity to support the targeting of fraudsters across England and Wales. This approach has proven highly effective. Over a five-year period, national intensification activity has resulted in 1,904 arrests, the seizure of assets valued at £45 million, and the completion of more than 2,000 voluntary interviews and cease-and-desist interventions.

These outcomes demonstrate the significant impact of coordinated national enforcement activity in disrupting fraud networks, removing criminal assets and protecting the public from harm.


POLICE PROFESSIONAL

ABOUT US CONTACT US MY ACC

NEWS FEATURES INVESTIGATIVE PRACTICE SHARING PRACTICE JOBS EVENTS EXCE

Operation Henhouse delivers strongest results yet in fifth year of national fraud crackdown

More than 550 arrests were made as part of Operation Henhouse, the fifth year of a UK-wide campaign against fraud.

Mar 24, 2026 By Paul Jacques

Operation Seraphim

The Fraud Targeting Cell, working in partnership with the Cyber Defence Alliance, developed and delivered Operation Seraphim, an innovative initiative targeting fraud facilitated through UK-focused Telegram channels.

Built on strong public and private sector collaboration, the operation combined intelligence and analytical expertise to disrupt criminal activity impacting both the UK and the global financial sector. Working alongside UK policing partners, the National Crime Agency and the Nigeria Police Force, the operation resulted in 31 arrests during the enforcement phase, with additional arrests made subsequently and further activity planned in both the UK and Nigeria.

Investigations uncovered serious, organised criminality extending beyond fraud, including money laundering, drug offences, weapons-related activity, document forgery, and wider organised crime. Significant criminal assets, fraudulent documentation, devices, and evidence of cyber-enabled offending were seized. Alongside enforcement action, a prevention campaign was delivered across targeted channels, with academic partners assessing its impact. Initial findings indicate a reduction of around 40% in engagement between users on the affected channels, demonstrating a clear and immediate disruption effect and highlighting the success of the operation in changing offender behaviour online.

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

FRAUD

National Protect Network

In 2024, the National Fraud Protect Network funding enabled the formation of a new network of Regional Protect Officers, co-ordinated centrally from within CoLP.

This network has now merged with the National Cyber Protect Network and resources within Report Fraud to form a National Protect Network that is aligned, makes best use of the data provided by Report Fraud and co-ordinates and supplies materials for a national campaign calendar.

In 2025, a National Protect Strategy was delivered through partnership working with UK Finance and is now being implemented across the network.

The pillars of the National Protect Strategy are underpinned by a governance and standards framework and are outlined below:-

- Education and Training – Ensuring the awareness we are raising is evidence based, sustainable and impactful and is reinforced by effective training.
- One Network, One Voice – aligning the Fraud and Cyber Protect Network including shared practices, tasking and creation of a consistent brand identity and content.
- Data and Intelligence – Proactive identification of vulnerability and prioritisation coupled with a framework to accurately identify our performance and influence.

The PROTECT Network has delivered the following key achievements: -

Project Aegis: Between February and September 2025, Project Aegis piloted a proactive, intelligence-led approach for preventing fraud victimisation, using a 'hot spotting' model. Officers and volunteers visited high risk neighbourhoods visiting 5,600 properties to distributed fraud prevention materials.

Operation Serrano: a Courier Fraud intensification initiative, to raise awareness amongst jewellers and taxi drivers about the growing trend of Courier Fraud and help them recognise and prevent victimisation.

Operation Tonic: a Romance Fraud intensification, aimed to raise awareness via posters displayed in high footfall areas.

We Will Enhance Victim Care and Support

FRAUD

The 2023 Strategy committed to improving victim care and support, with a focus on reducing the harm caused by fraud and cyber crime and preventing repeat victimisation.

A significant milestone towards achieving this objective was delivered through the Fraud Reform Programme, which funded the expansion of the National Economic and Cybercrime Victim Care Unit (NECVCU). The programme established dedicated new teams with the objective of extending Level 1 victim services nationally. This was the first strategic commitment to be fully achieved under the Strategy.

As a result, Level 1 victim services were successfully expanded to 43 police forces, providing a consistent baseline of support to victims across England and Wales. In addition, enhanced Level 2 services for vulnerable victims were also extended to 43 police forces, ensuring that those most at risk received tailored support and safeguarding interventions.



The launch of **Report Fraud** has enabled a further step change in victim care. The NECVCU teams have now been integrated into the wider Report Fraud Target Operating Model, creating a more cohesive victim support service and providing opportunities for further improvements in safeguarding, communication and service delivery.

We Will Enhance Victim Care and Support

FRAUD

Report Fraud Victim Services

Following the submission of a fraud or cyber crime report, victims are supported through the **Victim Services** function within Report Fraud. Specialist Victim Care Advocates undertake vulnerability assessments and provide support appropriate to the victim's circumstances, including:

- **Level 1 services** for non-vulnerable victims;
- **Level 2 services** for vulnerable victims requiring enhanced support; and
- **Level 3 referrals** for high-harm cases, which are directed to local police forces for further intervention.

In November 2025 they supported their **1,000,000th** victim. Preventing a total of **£13,972,168.00** from being lost to fraudsters through repeat victimisation. Returning a total of **£8,229,945.97** to victims

This approach ensures victims receive a consistent national standard of care and support, regardless of where they live. Support may include referrals to local policing teams, victim care partners, healthcare services, local authorities, charities and other specialist support organisations. Victim Services also manage urgent safeguarding responses, including requests for immediate police attendance where there are concerns relating to victim safety or risk of serious harm.

A significant improvement delivered through Report Fraud is the enhanced level of engagement available throughout the victim journey. Victims now benefit from more than 40 communication touchpoints across the service, providing greater transparency and reassurance. Through the Report Fraud portal, victims can monitor the progress of their report and receive direct updates on key developments and outcomes.

Victim Services is embedded throughout the end-to-end reporting process, ensuring support is available at every stage of the victim journey. Work is continuing to strengthen partnerships between policing and the third sector, with the aim of creating a seamless pathway between reporting, safeguarding and longer-term support services to help victims recover and reduce the risk of future victimisation.

MONEY LAUNDERING AND ASSET RECOVERY

Achievements

7 out of 8 deliverables have been achieved over the course of the strategy.

We have delivered:-

- **Uplift of 100 financial investigators** and intelligence professionals in the regions dedicated to increasing money laundering disruptions and assets seized from criminals
- **Asset Management Office** within CoLP
- **Anti-Money Laundering and Asset Recovery Intelligence Development Team;**
- **National Crypto Network – financial investigation teams** focused on disrupting crypto facilitated money laundering across the regional network.

AMLAR Programme

In 2023 the **Anti Money Laundering and Asset Recovery (AMLAR)** Programme launched, led by the Home Office this 3-year programme provided and extra £21.8 million of investment into policing to increase assets seized and recovered from criminals and disrupt more money laundering offenders.

The investment resulted in an extra 100 financial investigator and intelligence roles across Regional Economic Crime Units, and the delivery of national leadership and co-ordination of these teams centrally within CoLP.

In addition, two new national capabilities have been delivered;

A national **AMLAR Intelligence Development Team, and a National Asset Management Office.** Both of these were delivered in the final year, 25/26, and continue to develop their capabilities to support national policing to disrupt more money laundering criminals and seize more criminal assets.

Building on the original programme objectives, additional funding in 2025/26 enabled the creation of a **Crypto Financial Investigation Network**, with dedicated capability now established across every region.

As the use of cryptocurrency to facilitate money laundering continues to grow, these specialist teams play a vital role in keeping pace with evolving criminal methodologies. Leveraging new powers provided by the **Economic Crime and Corporate Transparency Act**, together with enhanced intelligence-sharing partnerships across the private sector, the network is transforming the response to crypto-enabled financial crime, helping to disrupt organised criminal activity and recover assets from those seeking to profit from crime.

Over the previous three years, the total amount of assets seized was £682,829,434 and victim compensation was £41,996,046

MONEY LAUNDERING AND ASSET RECOVERY

Deliverables

Improve outcomes for victims	Proactively pursue offenders	Protect people and businesses
We will increase criminal justice outcomes and disruptions against money laundering offenders.	We will increase intelligence led proactive operations and locally developed operations regarding money laundering offending linked to serious and organised crime, ensuring the relevant deconfliction safeguards are followed.	We will increase the understanding of money mules, and how they are recruited. This will include an assessment of pathways into other criminality and links to other areas of SOC.
We will seize and restrain more criminal assets through increased asset denial activity.	We will increase intelligence collected on the money laundering threat and record on the appropriate systems. We will task covert intelligence capabilities to collect money laundering intelligence in line with NECC set intelligence requirements	We will improve recording of money mule offending and use of low-level police interventions. Develop practice for a graduated policing response to repeat offenders.
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 as required.	We will ensure all OCGs and priority individuals have money laundering recorded within their criminality where applicable.	

Improve Outcomes for Victims

Ensuring that criminal assets are identified, seized and ultimately returned to victims is a core function of asset recovery teams across the UK. The **Anti-Money Laundering and Asset Recovery (AMLAR) Programme** has significantly strengthened this capability through sustained investment in specialist financial investigation and intelligence resources, enhancing the ability of policing to follow the money, disrupt criminal networks and prevent offenders from benefiting from their crimes.

A key element of the programme has been the growth of dedicated **Financial Investigators and intelligence specialists** across the regional network, increasing national capacity to investigate complex money laundering activity linked to fraud, cyber crime and organised crime. This enhanced capability has improved the identification and restraint of criminal assets, strengthened intelligence development and increased opportunities to secure confiscation orders and victim compensation.

Over the past three years, AMLAR-funded resources have enabled forces and Regional Organised Crime Units (ROCUs) to pursue increasingly complex financial investigations, ensuring that asset recovery activity remains an integral part of the policing response to economic crime.

Case Study: Operation Ruche and Operation Mille

The value of AMLAR-funded capability is demonstrated by the investigation into **Vincent Lebouf**, which uncovered a sophisticated criminal network involved in fraud, money laundering and large-scale cannabis cultivation. Building on intelligence developed through Operation Ruche, AMLAR-funded investigators identified shell companies and linked business accounts, creating opportunities for substantial victim compensation. Subsequent enquiries through Operation Mille revealed links between Lebouf, a network of property management businesses and numerous properties being used for cannabis cultivation across multiple force areas.

Working with partners including HMRC, NFIB, DVLA and HM Land Registry, investigators uncovered nine shell companies, more than 60 properties linked to criminal activity and evidence of conveyancing fraud and fraudulent property auction scams that generated losses exceeding **£9 million**. Financial investigation identified significant money laundering activity, including the purchase and rapid resale of luxury vehicles through business accounts. Enforcement action resulted in the arrest of Lebouf, searches across seven locations, and the seizure of vehicles and a speedboat valued at almost **£4 million**.

He was subsequently sentenced to **10 years' imprisonment**, with confiscation proceedings ongoing. The case demonstrates how AMLAR-funded expertise can uncover hidden assets, dismantle complex criminal structures and create meaningful opportunities for victim restitution.

Case Study: Operation Circus 2

AMLAR investment has also delivered tangible benefits for victims through its support to **Operation Circus 2**, a major Ponzi scheme investigation targeting elderly and vulnerable victims. Following the successful prosecution of the offenders, local capacity challenges threatened the force's ability to pursue complex confiscation proceedings. AMLAR-funded Financial Investigators within the ROCU were able to step in and lead the post-conviction asset recovery work on behalf of the force.

As a result, investigators have secured **eight POCA Confiscation Orders worth more than £3 million**, creating a significant opportunity to recover criminal proceeds and compensate victims. The largest order exceeded **£1.2 million**, with further proceedings still underway representing an additional pipeline value of more than **£3 million**. This case highlights the critical role AMLAR funding plays in ensuring that specialist financial investigations continue despite local resourcing pressures, helping to maximise asset recovery, support victims and reinforce the principle that crime should never pay.

Collectively, these achievements demonstrate how AMLAR funding has transformed the policing response to money laundering and asset recovery. By increasing specialist capacity, strengthening intelligence development and supporting complex investigations, the programme has improved the ability of law enforcement to identify and recover criminal assets, disrupt organised crime networks and deliver better outcomes for victims of fraud and economic crime.

Asset Management Office

The **Asset Management Office (AMO)** is being established to provide a coordinated national approach to the management, preservation and disposal of seized and restrained criminal assets across policing and wider law enforcement. The AMO is designed to improve consistency, governance and value for money, while ensuring that both physical and digital assets are managed effectively throughout the asset recovery process.

Since its inception, the AMO has made significant progress in laying the foundations for national delivery. Key achievements include supporting the development of the new **Asset Recovery IT (ARIT)** system, launching a national Knowledge Hub and website, providing operational support on complex asset recovery investigations, establishing partnerships across UK law enforcement and international asset management organisations, and influencing policy and legislative reform to improve asset management powers. The AMO has also commenced work on a national procurement framework and developed its strategic mission, vision and operating model.

Looking ahead, the AMO will focus on strengthening national capability through practitioner training, publishing guidance and standards, implementing national asset management processes, supporting the rollout of ARIT, expanding its operational support function, and assuming responsibility for the management of both physical and crypto assets. Subject to funding approval, the AMO is expected to become fully operational alongside the wider national asset recovery reforms planned for 2027.

AMO
ASSET MANAGEMENT OFFICE

NECC
NATIONAL ECONOMIC CRIME CENTRE
A multi-agency unit housed in the NCA NCA

MONEY LAUNDERING AND ASSET RECOVERY

Proactively Pursue Offenders

Report Fraud | CITY OF LONDON POLICE

A key priority over the past three years has been a strategic shift towards the **proactive identification and disruption** of money laundering offenders through intelligence development and the targeting of criminal business enablers. Rather than relying solely on reactive investigations, the programme has invested in specialist intelligence capabilities that identify emerging threats, uncover previously unknown offenders and develop opportunities for enforcement action.

The **SARS Intelligence Development Team (IDT)** was established as a national network in 2021 to proactively exploit financial intelligence submitted through the Suspicious Activity Reports (SARs) regime. The team analyses and develops intelligence to identify criminality, support investigations and enable law enforcement interventions. Since its inception in 2020, the SARS IDT has recovered assets valued at more than £6 million and has disseminated 855 intelligence packages to policing teams across the UK. Current areas of focus include criminality linked to the illicit sale of weight loss drugs, prostitution and fraud, demonstrating the team's ability to identify and respond to evolving threats.

Building on this successful model, the **AMLAR Intelligence Development Team (IDT**) was established in 2024 to provide a specialist capability dedicated to identifying, understanding and disrupting money laundering associated with fraud and cyber crime. Operating across force, regional and national boundaries, the team develops actionable intelligence that supports the identification of high-harm offenders, maps criminal networks and targets the financial infrastructure that enables economic crime.

Since August 2025, the **AMLAR IDT** has produced and disseminated 73 subject profiles to Regional Organised Crime Units (ROCUs), providing intelligence that supports operational activity, investigative opportunities and asset recovery interventions. By progressing intelligence packages that may not otherwise be developed through local resources alone, the team is enhancing the national response to money laundering and strengthening law enforcement's ability to pursue offenders and disrupt organised criminality.

The AMLAR IDT is also working closely with the **National Economic Crime Centre (NECC) Data Fusion capability**, combining intelligence, data analytics and partner insights to build a more comprehensive understanding of money laundering threats. This collaboration is improving the identification of emerging trends, strengthening the mapping of criminal networks and enabling better coordinated activity across the economic crime landscape. Together, these capabilities ensure that intelligence is translated into tangible operational outcomes, driving a more **proactive and intelligence-led** approach to pursuing money laundering offenders.

Proactively Pursue Offenders

Enhancing the Recovery of Criminal Crypto Assets

As criminals increasingly adopted cryptocurrencies to launder the proceeds of crime, law enforcement faced a new challenge that required specialist skills, technology and legal powers. Over the past three years, significant investment through the **AMLAR Programme**, alongside legislative changes introduced by the **Economic Crime and Corporate Transparency Act 2023**, has transformed policing's ability to identify, seize and recover crypto assets. A key milestone was the NPCC-led national procurement of blockchain analytics tools, which secured access to world-leading **cryptocurrency investigation capabilities** for forces and Regional Organised Crime Units (ROCUs) across England and Wales. Combined with the establishment of a dedicated Crypto Asset Seizure Network in every region, policing now has enhanced capacity to trace illicit cryptocurrency transactions and target criminal assets.

Although national recording arrangements will not be fully mature until the introduction of the ARIT system in 2027, available data from the crypto storage facility and regional teams demonstrates substantial growth in cryptocurrency seizures and recoveries, reflecting both increased criminal use of crypto-assets and improved law enforcement capability. Investment in specialist skills has also been central to this progress. In 2025, the NPCC Cybercrime Team, in partnership with TRM Labs, launched the **Cryptocurrency Tactical Advisor and Seizure Course**, developed in response to the growing use of cryptocurrency in serious crime, including kidnap and extortion offences. The programme was supported by the publication of a **National Cryptocurrency Seizure Standard Operating Procedure**, providing a consistent framework for operational activity.

By the end of 2025/26, 90 officers and staff had completed advanced **Cryptocurrency Tactical Advisor (CTA) and seizure training**, establishing a network of specialists across all regions. This capability ensures that forces can access expert advice and operational support when dealing with cryptocurrency-related investigations, strengthening the overall response to crypto-enabled money laundering and helping to deprive offenders of their criminal profits.

NECC
NATIONAL ECONOMIC CRIME CENTRE
A multi-agency unit housed in the NCA

National Intensifications

MONEY LAUNDERING AND ASSET RECOVERY

Operation Machinize: Targeting Money Laundering on the High Street

A significant example of the programme's proactive approach to pursuing money laundering offenders is its support to **Operation Machinize**, a National Economic Crime Centre (NECC) led national intensification focused on criminal groups using **cash-intensive high street businesses** to launder the proceeds of crime. Working alongside police forces, Regional Organised Crime Units (ROCUs) and partner agencies, financial investigators and the AMLAR Intelligence Development Team (IDT) have helped identify, develop and target businesses suspected of being used as fronts for money laundering and wider organised criminality.

The operation has demonstrated how intelligence-led activity can identify criminal business enablers and disrupt the financial infrastructure that supports organised crime. Two national phases of Operation Machinize have targeted barbershops, vape stores, nail bars, car washes and other cash-intensive businesses linked to money laundering, drug trafficking, organised immigration crime, modern slavery and illicit tobacco sales.

The first phase of the operation resulted in 35 arrests, over £1 million in frozen bank accounts, the execution of more than 80 warrants, the seizure of criminal cash and illicit goods, and the safeguarding of individuals potentially vulnerable to modern slavery. The second phase expanded nationally, involving every UK police force and ROCU, leading to 924 arrests, the seizure of over £10.7 million in suspected criminal proceeds and the disruption of thousands of businesses linked to economic crime and the shadow economy.

Operation Machinize highlights the value of proactive intelligence development, cross-agency collaboration and targeted financial investigation in identifying offenders, disrupting criminal networks and preventing the abuse of legitimate businesses for money laundering purposes. This has now evolved into a **High Street Taskforce** that will undertake this activity continuously over the next two years.

Report Fraud | CITY OF LONDON POLICE

BBC NEWS
Home | UK | World | Business | Culture | Politics | Health | Tech | InDepth | BBC Verify
England | Local News

Police raid barbers and vape shops suspected of being fronts for crime gangs



Police raided 265 businesses, including barbers, mini-marts and vape shops

INDEPENDENT
NEWS | PREMIUM | SPORT | VOICES | CULTURE | LIFESTYLE | INDYBEST

Barbers and vape stores among 2,700 high street shops raided in money-laundering crackdown

These extensive raids – the UK's largest ever crackdown of its kind on money laundering – form the second stage of Operation Machinize

Margaret Davis
Tuesday 11 November 2025 07:37 GMT



The National Crime Agency (NCA) concluded that a critical "tipping point" had been reached when it came to money laundering (Aaron Chown/PA)

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

AMLAR's Protect People and Businesses deliverables have focused on strengthening the national response to the growing threat posed by money mule activity. Money mules play a critical role in the movement of criminal funds, enabling fraudsters and organised crime groups to transfer money beyond the reach of law enforcement and financial institutions. However, the harm caused by money mule activity extends well beyond financial loss.

The recruitment of money mules frequently involves the grooming and exploitation of vulnerable adults and children, who are persuaded, coerced or manipulated into allowing their bank accounts to be used for criminal purposes. In many cases, individuals are unaware of the consequences of their actions and can find themselves drawn into wider criminality. In addition, victims of fraud can unknowingly become part of a chain of mule accounts as stolen funds are moved through the banking system.

Money Mules Threat Assessment

A Money Mules 4P Plan was developed and published by the AMLAR Intelligence Development Team on 30 March 2026 to provide forces with a structured framework for tackling money mule activity through the four pillars of Pursue, Prevent, Protect and Prepare.

The plan has increased awareness and understanding of the threat across policing and has been adopted by a growing number of forces to support local and regional responses. As a living document, the plan continues to evolve, incorporating emerging intelligence, operational learning and best practice to ensure it remains relevant and effective in addressing the changing nature of money mule activity and the wider criminality it enables.

A strategic decision was made to focus on Money Mule Herders and not Money Mules by System Prioritisation strategic governance group (NCA/FCA). This has changed the approach, and the AMLAR IDT in the City of London Police have worked closely with the financial sector to design a framework of how to effectively disrupt and pursue money mule networks.

We are currently in a pilot phase of receiving packages from banks after they have collated accounts through ECCTA sharing in the prate sector and work is nearing the start of a pilot to receive the top 100 pooling accounts as indicated by VocaLink (Mastercard) with ThreatMetrix data incorporated.

This work will be re-instated under the new Prevent workstream being delivered by the Fraud Strategy 2026 –2029.

Achievements

100% of the cyber deliverables have been completed over the past three years.

Over the reporting period, the Cyber Portfolio has continued to mature its nationally coordinated response to cyber crime, delivering improvements across the Pursue, Protect and Prevent agendas. Through the **Nationally Led, Regionally Managed, Locally Delivered (NLRMLD)** model, investment in enhanced governance, intelligence capabilities and the introduction of the new Report Fraud service has strengthened the identification, investigation and disruption of cyber offenders, while improving the service provided to victims.

Proactive operational activity has also expanded through initiatives such as **Project Capstone**, which has supported the identification of cyber criminals operating through cryptocurrency and Dark Web platforms and contributed to the seizure of more than £40 million in criminal assets. Enhanced blockchain analytics capabilities have further enabled the identification of high-harm offenders and substantial asset recovery opportunities.

Alongside this enforcement activity, the Cyber Portfolio has significantly strengthened national cyber resilience. The **Cyber Resilience Centre Network** now supports more than 31,000 businesses and organisations, providing trusted, police-led cyber security advice and preventative services, while **Police CyberAlarm** has grown to over 8,500 member organisations and identified more than one billion suspicious cyber events.

The **Cyber Choices** programme continues to divert individuals away from cyber offending, supported by the introduction of the Cyber Offender Risk Assessment (CORA) framework, which provides an evidence-based approach to measuring intervention effectiveness.

These efforts are further enhanced by the **Specialist Crime Volunteer Network**, which provides policing with access to specialist cyber, digital and data expertise from industry and academia. Collectively, these initiatives have strengthened the ability of policing to pursue offenders, protect individuals and organisations from cyber threats, and build a more resilient national cyber crime capability.

THE CYBER RESILIENCE CENTRE NETWORK

POLICE CYBERALARM

SCVN
SPECIALIST CRIME VOLUNTEER NETWORK
Operated by City of London Police



Deliverables

Improve outcomes for victims	Proactively pursue offenders	Protect people and businesses
We will ensure that forces and regions have sufficient resources in place to effectively deal with the threat of cyber in accordance with the Strategic Policing Requirement and the NPCC Cyber Portfolio Target Operating Model, Tactical Action Plan and National Performance Framework.	We will increase intelligence led proactive operations and self development operations regarding CMA offending, ensuring the relevant deconfliction safeguards are followed.	We will deliver NCSC agreed or consistent content across the PROTECT network, to ensure consistent messaging against HMG guidance and promoting HMG systems and services.
We will increase the policing response and outcomes linked to NFIB / FCCRAS crime dissemination packages. We will ensure full and timely compliance to from forces to record disseminations from the National Fraud Intelligence Bureau (NFIB) appropriately and that subsequent outcomes are reported back to NFIB correctly.	We will register all cyber related intelligence on the appropriate intelligence systems. We will capture and disseminate operational summaries for key cyber crime operations, subject details, associates, identifiers, MO etc. Including the implementation of a closing report system across ROCUs and forces, for all cyber operations. We will secure national intelligence capability that enables the delivery of intelligence and operational tools.	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.
		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.
		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.

Improve Outcomes for Victims

The Cyber Portfolio has continued to strengthen the policing response to cyber crime and fraud, with a clear focus on improving outcomes for victims through enhanced governance, performance management and investigative capability. Following the introduction of the **Nationally Led, Regionally Managed, Locally Delivered (NLRMLD)** model, significant progress has been made in aligning governance arrangements, establishing clearer accountability and driving greater consistency in service delivery across the network. Continued oversight and refinement have enabled the development of meaningful success measures, supporting a more agile, responsive and nationally coordinated cyber policing capability.

Alongside these structural improvements, investment in national reporting and intelligence capabilities has enhanced the ability of policing to identify investigative opportunities and better support victims.

The introduction of the new **Report Fraud** service represents a significant step forward, providing a modernised reporting platform that improves the quality of information captured from victims, supports more effective crime assessment and enables faster identification of linked offending and emerging threats.

This improved intelligence picture strengthens the ability of law enforcement to pursue offenders and maximise opportunities for positive victim outcomes.

These developments are reflected in the outcomes achieved by teams across the **Tackling Cyber UK (TCUK)** network. Between 2022/23 and 2025/26, arrests and cautions increased from **315 to 378**, while charges rose from **119 to 145**. The use of community resolutions and other positive outcomes also increased significantly, from **40 to 110**, demonstrating an increased ability to identify proportionate interventions and deliver tangible results.

Despite the complexity and often international nature of cyber-enabled offending, convictions remained consistently strong, with **103 convictions achieved in 2025/26**.

Collectively, these improvements demonstrate how a more coordinated national approach, supported by enhanced reporting capabilities, stronger governance and improved performance management, is enabling policing to deliver better investigative outcomes, increase offender accountability and provide a more effective service to victims of cyber crime and fraud.

Team Cyber UK National Outcomes Data

	22/23	23/24	25/26
Arrests / Caution	315	364	378
Charged	119	137	145
Cautions	40	44	45
Community Resolutions and Outcome 21 & 22	40	81	110
Convictions	109	92	103

Proactively Pursue Offenders

The Cyber Portfolio has continued to strengthen its proactive approach to identifying and disrupting cyber criminals by combining law enforcement capabilities with specialist expertise from the private sector. This approach recognises that many cyber and cyber-enabled offenders operate across the Dark Web and cryptocurrency ecosystems, requiring innovative methods to identify offenders, trace criminal assets and develop enforcement opportunities.

A key example of this approach is **Project Capstone**, a public-private partnership established in September 2024 with leading cryptocurrency analytics providers. The initiative focuses on identifying criminals involved in cyber and cyber-enabled crime through the exploitation of blockchain intelligence, cryptocurrency transactions and Dark Web activity. Since its inception, Project Capstone has delivered significant results, identifying high-harm offenders and supporting the seizure of criminal assets valued at **more than £40 million**.

Building on this success, the NPCC Cybercrime Team has secured enhanced blockchain analytics capability through partnerships with industry-leading providers, including Chainalysis, TRM and Elliptic.

These specialist capabilities have generated substantial operational intelligence, leading to the identification of more than **15 UK-based Dark Web drug vendors** and the development of asset confiscation opportunities valued at over **£30 million**. By combining advanced analytics with law enforcement intelligence, the programme is enabling investigators to identify offenders who would otherwise remain hidden within anonymised online environments.

Recognising the increasing convergence between the Dark Web, cryptocurrency and wider online serious and organised crime (OSOC), work has also progressed to establish a new regional prioritisation and coordination framework.

The model will provide enhanced oversight of operational activity and support the effective assessment, prioritisation and dissemination of intelligence received through law enforcement and private-sector partnerships. Scheduled for implementation in 2026/27, this new governance structure will strengthen the national ability to identify emerging threats, coordinate operational activity and target the criminals and networks responsible for online offending.

Together, these developments demonstrate a significant shift towards proactive, intelligence-led cyber policing. By leveraging specialist technology, commercial partnerships and coordinated operational activity, the Cyber Portfolio is improving the identification of cyber offenders, increasing opportunities for asset recovery and disrupting the criminal networks that operate across the digital landscape.

Cyber Choices

The **Cyber Choices** programme continues to play a key role in preventing individuals, particularly young people and those at risk of offending, from becoming involved in cyber-dependent crime. By identifying and engaging individuals at an early stage, the programme provides tailored interventions that address risk factors, promote positive pathways and reduce the likelihood of future offending.

To strengthen this approach, the Cyber Portfolio's **Cyber Offender Risk Assessment (CORA)** framework has now been embedded into professional practice across all Prevent staff. Assessments are completed both before and after interventions, enabling robust analysis of offender risk profiles and intervention outcomes. This provides a strong evidence base to support ongoing evaluation, measure effectiveness and inform continuous improvement. Delivery and outcomes are monitored by the NPCC Cyber Portfolio and are currently being reviewed to ensure the framework continues to support effective, evidence-led prevention activity across the network.

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

A key objective of the Cyber Portfolio has been to reduce the harm caused by cyber crime by improving the cyber resilience of businesses, communities and public sector organisations. This has been achieved through a combination of prevention activity, partnership working, threat identification and the provision of practical support designed to help organisations better protect themselves from cyber threats.

The Cyber Resilience Centre Network and **Police CyberAlarm** demonstrate how the Cyber Portfolio is adopting a proactive, prevention-focused approach to protecting people and businesses. By combining trusted advice, industry expertise, threat monitoring and targeted interventions, the portfolio is helping organisations improve their resilience, reduce vulnerability to cyber crime and build a safer digital environment across England and Wales.

Cyber Resilience Centres

At the centre of this approach is the **Cyber Resilience Centre (CRC) Network**, a unique collaboration between law enforcement, government, academia and the private sector, delivering tailored cyber resilience support across nine regions in England and Wales. The network combines policing's expertise in crime prevention with the technical knowledge and resources of industry partners, providing trusted, police-led cyber security advice in an increasingly complex and unregulated marketplace.

The CRC Network underwent significant transformation during 2025/26, moving from a model of independently operated companies to a centrally governed structure under police leadership. This change has strengthened governance, improved consistency across regions and enhanced the network's ability to deliver prevention activity at scale. As a result, membership has continued to grow significantly, reaching **31,374 businesses and organisations by March 2026**, representing an increase of approximately **12,000 members during the year**.

The network's reach and impact have been further strengthened through the expansion of the **National Ambassador Programme**, with 17 major organisations now supporting the initiative. These partnerships provide funding, expertise and access to industry insights, enabling the CRCs to deliver targeted awareness campaigns and practical support to small and medium-sized enterprises (SMEs). Research delivered through the programme has also helped shape the national understanding of cyber risk and informed government thinking on improving the communication of cyber security advice to businesses and supply chains.

The CRCs continue to provide direct support to organisations seeking to improve their cyber resilience. Feedback from businesses demonstrates the tangible benefits of this support, helping organisations recover from cyber incidents, strengthen security practices and work towards recognised standards such as **Cyber Essentials**. This preventative approach reduces vulnerability to attack while supporting long-term resilience across critical sectors and local economies.

Police CyberAlarm

The **Police CyberAlarm (PCA)** service has become an increasingly important national capability for protecting organisations from cyber threats. The service provides free monitoring software which enables businesses to identify malicious activity targeting their networks and take preventative action before attacks can succeed. Since its launch, CyberAlarm has identified **over one billion suspicious events**, helping organisations reduce their exposure to cyber threats while also providing valuable intelligence to support law enforcement activity.

During 2025/26, CyberAlarm continued to expand, with membership increasing from **6,362 to 8,555 organisations**, representing **34.5% year-on-year growth**. The service was integrated into the national Protect network, strengthening its role as a coordinated cyber prevention capability. Operational activity included **312 member engagements** and the dissemination of **2,275 geo-located IP notification packs**, enabling organisations to identify and address cyber risks associated with activity detected within their networks.