Public Document Pack

CITY OF LONDON

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

Date: **FRIDAY, 13 MAY 2022**

Time: 11am

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

Members:
Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chairman)
Alderman Professor Emma Edhem
Alderman Timothy Hailes
Andrew Lentin (External Member)
James Tumbridge
Chris Hayward, Chair, Policy & Resources Committee (Ex-Officio Member)
Dawn Wright
Michael Landau (External Member)
Deputy Graham Packham

Enquiries: **Polly Dunn**
tel. no: 020 7332 3726
polly.dunn@cityoflondon.gov.uk

Accessing the virtual public meeting

Members of the public can observe this virtual public meeting at the below link:
https://youtu.be/cFDF6CFU5rk

A recording of the public meeting will be available via the above link following the end of the public meeting for up to one municipal year. Please note: Online meeting recordings do not constitute the formal minutes of the meeting; minutes are written and are available on the City of London Corporation’s website. Recordings may be edited, at the discretion of the proper officer, to remove any inappropriate material.

John Barradell
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

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

3. **TERMS OF REFERENCE**
To receive the terms of reference of this Committee, as agreed by the City of London Police Authority Board at its meeting of 25 April 2022.

For Information
(Pages 5 - 6)

4. **MINUTES**
To agree the public minutes and non-public summary of the meeting held on 14 February 2022.

For Decision
(Pages 7 - 12)

5. **PUBLIC OUTSTANDING REFERENCES**
Joint report of the Town Clerk and Commissioner.

For Information
(Pages 13 - 16)

6. **NATIONAL LEAD FORCE UPDATE**
Report of the Commissioner.

For Information
(Pages 17 - 24)

7. **CYBER GRIFFIN UPDATE**
Report of the Commissioner.

For Decision
(Pages 25 - 28)

8. **Q4 NATIONAL LEAD FORCE PERFORMANCE UPDATE**
Report of the Commissioner.

For Information
(Pages 29 - 44)

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

For Information
(Pages 45 - 50)

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

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

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

For Decision

Part 2 - Non-Public Agenda

13. **NON-PUBLIC MINUTES**
To agree the non-public minutes of the meeting held on 13 February 2022.

For Decision
(Pages 51 - 52)

14. **NON-PUBLIC OUTSTANDING REFERENCES**
Joint report of the Town Clerk and Commissioner.

For Information
(Pages 53 - 54)

15. **NATIONAL LEAD FORCE PLAN 2020-23- REFRESH**
Report of the Commissioner.

For Information
(Pages 55 - 86)

16. **NPCC CYBER CRIME PORTFOLIO UPDATE**
Report of the Commissioner.

For Information
(Pages 87 - 90)

17. **STAKEHOLDER ENGAGEMENT PLAN- ECONOMIC AND CYBER CRIME**
Report of the Commissioner.

For Discussion
(Pages 91 - 114)

18. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE - NEXT GENERATION AND CURRENT SERVICE UPDATE REPORT**
Report of the Commissioner.

For Information
(Pages 115 - 150)

19. **CITY OF LONDON POLICE STAFF SURVEY'S- FUTURE APPROACH**
Report of the Commissioner.

For Information
(Pages 151 - 166)

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

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

Economic and Cyber Crime Committee
Composition

- Up to six Members of the Police Authority Board appointed by the Police Authority Board (in addition to the Chair and Deputy Chair of the Board).
- Up to two co-opted Court of Common Council Members to be appointed by the Police Authority Board.
- Chair and one other Member of the Policy and Resources Committee, to be appointed by that Committee.
- Up to two external Members, to be appointed by the Police Authority Board.

Frequency of meetings
The Committee shall meet four times per annum.
.
Quorum
Three Members (of which at least two must be Common Councillors).

Terms of Reference
To be responsible for:

a) overseeing the force's national responsibilities for economic, fraud and cyber crime, having regard to the strategic policing requirement and relevant national strategies in this area;

b) monitoring government, and other external agencies' policies and actions relating to economic and cyber crime;

c) overseeing the delivery of the City's economic and cyber crime strategies, programmes, projects and other relevant improvement plans including (but not limited to) the National Lead Force Plan, Strategic Communications and Engagement Plan, NPCC Cyber Crime Programme, Cyber Griffin and Fraud and Cyber Reporting & Analysis Service Programme;

d) overseeing the City of London Police's private sector partnerships with regard to fraud, economic and cyber crime;

e) identifying and overseeing opportunities to exploit the synergies between the Corporation's Cyber Security agenda and that of the City of London Police;

f) overseeing the business strategy, service and financial performance of the Economic and Cyber Crime Academy;

g) making recommendations to the Police Authority Board in any other matters relating to economic and cyber crime.

This page is intentionally left blank

ECONOMIC AND CYBER CRIME COMMITTEE OF THE CITY OF LONDON POLICE AUTHORITY BOARD
Monday, 14 February 2022

Minutes of the meeting of the Economic and Cyber Crime Committee of the City of London Police Authority Board held at Committee Rooms, 2nd Floor, West Wing, Guildhall on Monday, 14 February 2022 at 2.00 pm

Present

Members:
Deputy James Thomson (Chair)
Deputy Keith Bottomley
Deputy Graeme Doshi-Smith
Alderman Bronek Masojada
Catherine McGuinness (Ex-Officio Member)
Dawn Wright
Landau (External Member)

Officers:

Peter O'Doherty	-	Assistant Commissioner, City of London Police
Chris Bell	-	City of London Police
Clinton Blackburn	-	City of London Police
Simon Latham	-	Director, Police Authority Team
Alix Newbold	-	Interim Director, Police Authority Team
Oliver Bolton	-	Deputy Head, Police Authority Team
Polly Dunn	-	Town Clerk's Department
Andrew Buckingham	-	Town Clerk's Department
Giles French	-	Innovation & Growth Department

1. **APOLOGIES**
Apologies were received from Tijs Broeke, Alderman Professor Emma Edhem, Alderman Tim Hailes. Andrew Lentin was observing online. Michael Mitchell, external Member of the Professional Standards and Integrity Committee, was also observing virtually.

Sir Craig Mackey attending in person to observe the meeting.

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

3. **MINUTES**
RESOLVED, that the public minutes and non-public summary of the meeting held on 4 November 2021, be approved as an accurate record.

4. **PUBLIC OUTSTANDING REFERENCES**

Members received a report of the Town Clerk and Commissioners regarding the Committee’s outstanding references.

5. **Q3 NATIONAL LEAD FORCE PERFORMANCE REPORT**

Members received a report of the Commissioner regarding the Quarter 3 National Lead Force Performance.

There was a discussion on the issue of time taken to answer calls and the link between that and abandoned calls. 30% abandoned calls was considered high. A push toward guiding people to online reporting tools was necessary, to leave the call handlers free to speak to those who needed to (repeat victims, the elderly and vulnerable). Capacity was being built within the contact centre. As part of the user experience, callers would be assured there would be a handler waiting to speak to them when they got through.

There had been an attrition of staff within the contact centre which had impacted the call answering time. If at full staffing capacity, the numbers would improve.

The Chat Bot had managed 800hours (4FTEs) worth of reporting. It was about to commence its second iteration and was proving successful.

Further information was sought on the 50% of reports that don’t meet the target response date of 28 days. For example, were they dropped? When was the next target date for resolution?

Within the report there was no reference to the number of businesses that had reported fraud as a distinct data set to individuals who had reported. This would be an enhanced tool available in the Next Gen service.

There was concern that there was a perception of the public that by reporting, there would not be a reduction in crime. The positive outcomes of the work of the service needed to be reported through the right channels.

Where victims of crime were reporting cases of economic crime, the as NLF, COLP wanted to be as efficient as possible at identifying those where significant funds would be lost or making links to organised crime. It would then be for the local police force to investigate. There was a misconception by those using the service on this point.

The Force wished to maximise prevention and investigation.

Continuous improvement measures were in place for the Cyber Desk, to attract the best individuals to deal with reports from businesses. To triage these report and allocate to the most appropriate organisations to follow up.

Certain parts of the form were to be mandatory for completion, to reduce the need to follow up with the reporter.

There was a brief discussion on the Economic Crime Plan and Economic Crime Bill and Online Safety Bill. An Engagement Plan was requested.

On outcome two, there was a settlement from the spending review which would roll out to many more forces. The ambition was to level up all forces in England and Wales. Members sought more victim stories to help drive this work.

RESOLVED, that the report be noted.

6. **NATIONAL LEAD FORCE UPDATE**

Members received a verbal report of the Assistant Commissioner regarding National Lead Force.

Members heard about the renewal of an arrangement with Microsoft and suggested that the Force seek to do similar with other such as Amazon, PayPal and Google.

Social media companies had a duty of care as outlined in the Online Safety Bill. The Force was trying to be proactive in encouraging large, data rich, organisations to share their data to help improve the Force's ability to prevent and investigate cyber crime.

A discussion was had on the involvement of COLP with insurance companies, primarily on the need to improve the messaging so that these companies knew who to speak to when there was a cyber threat. The Chair of Policy and Resources supported the idea of improving this. She felt that UK Finance would be a good forum to raise this and suggested a round table for insurers be held (**1/2022/P**).

RESOLVED, that the update be noted.

7. **CYBER GRIFFIN UPDATE**

Members received a report of the Commissioner on Cyber Griffin.

There was support expressed for the use of POCA funds on Cyber Griffin.

Members wished to understand the breadth, depth and reach of this activity. What volume of services had been provided to what sectors, and where? (**2/2022/P**)

RESOLVED, that the report be noted.

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

Members received a report of the Director of Innovation and Growth, on the Department's activities related to Cyber and Economic Crime.

The Chair of Policy and Resources explained that she had started holding informal meetings with Police to see what work was being done to push the competitiveness agenda.

Some ‘blue sky’ thinking on the Centre for Cyber Excellence was sought (**3/2022/P**).

RESOLVED, that the report be noted.

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

There was a question on the campaigning undertaken for the Online Safety Bill.

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

There was no urgent business.

11. **EXCLUSION OF THE PUBLIC**

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

12. **NON-PUBLIC MINUTES**

RESOLVED, that the non-public minute of the meeting held on 4 November 2021, be approved as an accurate record.

13. **NON PUBLIC OUTSTANDING REFERENCES**

Members received a report of the Town Clerk and Commissioner regarding the Committee’s Non-Public Outstanding References.

14. **CONCENTRIX EXTENSION - COSTED ROADMAP**

Members received a report of the Commissioner regarding the Concentrix Extension and Costed Roadmap.

15. **STAKEHOLDER ENGAGEMENT AND POLICY UPDATE**

Members received a report of the Commissioner regarding Stakeholder Engagement and Policy.

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

There were no questions.

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

There was no other business.

The meeting ended at 15.40

Chairman

Contact Officer: Polly Dunn
tel. no: 020 7332 3726
polly.dunn@**cityoflondon.gov.uk**

This page is intentionally left blank

Agenda Item 5

ECONOMIC CRIME COMMITTEE – PUBLIC REFERENCES

12/2021/P	**4 November 2021** Innovation & Growth	By utilising the City and Mayoralty's convening power there would be better engagement with smaller FinTech firms. It was suggested that a FinTech specific event could be arranged.	Assistant Commissioner/ Dir for Innovation and Growth	**In progress** To be discussed with the Lord Mayor in the coming months.
1/2022/P	**14 February 2022 Item 6- National Lead Force Update**	A discussion was had on the involvement of COLP with insurance companies, primarily on the need to improve the messaging so that these companies knew who to speak to when there was a cyber threat. The Chair of Policy and Resources supported the idea of improving this. She felt that UK Finance would be a good forum to raise this and suggested a round table for insurers be held.	Commissioner of Police	**In Progress-** The City Police's ABI funded insurance investigation team have been asked to engage with CyberGriffin to explore opportunities
2/2022/P	**14 February 2022 Item 7- Cyber Griffin Update**	Members wished to understand the breadth, depth and reach of this activity. What volume of services had been provided to what sectors, and where?	Commissioner of Police	**Complete-**Update below ***Service volume* –** To date and excluding bespoke presentations, CyberGriffin(CG) have delivered 423 Baseline Briefings, 108 Table Top exercises, 52 Cyber Capability Assessment engagements and 28 Incident Response Training sessions. 'Awareness' is therefore CG's key deliverable as this is the focus of the Baseline Briefing. Notwithstanding the above statistics, it is important to note that the lower frequency services generally deliver a more lasting impact. Cyber Capability Assessments leave organisations with detailed plans for security improvements and often

				trigger changes in their security policy. Similarly, incident response training sessions often drive amendments to an organisations IR plan. Overall, CG supervisors believe that volume is still the better measure of impact given the amount of awareness CG deliver. CG believes that the lower frequency exercises run a closer second place than the statistics above suggest however. ***Sectors –*** Most of CG's engagement activity is with financial services. In the first years of the programme CG relied on survey data to confirm this but that data is based on those who feedback which is a fraction of the number that CG engages with. For the last 18 months CG have maintained a far more detailed record of their engagements. CG state they would not be able to extract a sector breakdown in the time they have before the next ECCC meeting but can provide a detailed sector based analysis for the next meeting if the ECCC want this information? If that is the case, any direction on which sectors are of interest would be helpful ahead of the team reviewing the data.

				Where – Originally, Cyber Griffin was totally Square Mile based and replied fully on physical presentations. Today, while the focus is organisations in the City, CG do far more work outside than previously through the use of the digital platform. Two key factors have driven this shift; Firstly, organisations seek a consistent security posture which means that assisting them requires Cyber Griffin to train people in that organisation wherever they are. CG regularly deliver briefings to other parts of the world where the organisation has a footprint in the City. Secondly, among protect teams Cyber Griffin has developed a specialist business focus, this means that other protect teams will refer more complex business engagements to them. This has been a source of increasing national work
3/2022/P	**14 February 2022 Item 8- Innovation and Growth update of Cyber and Economic Crime related activities**	The Chair of Policy and Resources explained that she had started holding informal meetings with Police to see what work was being done to push the competitiveness agenda. Some 'blue sky' thinking on the Centre for Cyber Excellence was sought	Dir Innovation and Growth / Private Secretary to the Chair of Policy	This action will need to be progressed in light of the new Chairmanship of Policy & Resources.

This page is intentionally left blank

Committee: Economic and Cyber Crime Committee	**Dated:** 13 May 2022
Subject: National Lead Force Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1,10, 12
Does this proposal require extra revenue and/or capital spending?	**N**
If so, how much?	**NA**
What is the source of Funding?	**NA**
Has this Funding Source been agreed with the Chamberlain's Department?	**NA**
Report of: Commissioner of Police Pol 23-22	**For Information**
Report author: AC Pete O'Doherty; Cdr Nik Adams Office of National Co-ordinator for Economic and Cyber Crime	

SUMMARY

This report provides information on key activities delivered as part of the National Lead Force Plan. These activities include:

- Improvements to Action Fraud reporting
- National protect campaigns to tackle online shopping and romance fraud
- Continued coordination of Project Otello activity
- Multiple arrests for courier fraud
- Force and PCC engagement

Recommendation(s)

It is recommended that members note the contents of this report.

MAIN REPORT

BACKGROUND

The National Lead Force Plan was approved by Police Authority Board in October 2020. The plan is structured around 5 key outcomes / aims with milestones and performance measures attributed to each milestone. This report will be a standing agenda item in future and will provide an overview of ongoing activity.

CURRENT POSITION

<u>Outcome 1: The public has confidence in the Action Fraud reporting service</u>

Action Fraud is the National Fraud and Cybercrime Reporting Service delivered by COLP. Responsibilities include providing a first point of contact for victims of fraud, crime reporting and triage. We constantly seek opportunities to improve the quality of service delivered informed by user feedback. A number of activities are in progress including changes to staffing and recruitment models and technological improvements.

Next Generation service project update

1. The Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) programme is implementing a transformational change.

   The future system will have an ability to ingest, analyse and publish information in a timely manner at scale to help the City of London Police (CoLP), in conjunction with forces across England, Wales and Northern Ireland, better prepare for the ever-evolving fraud and cybercrime landscape.

   Using automation across law enforcement, government agencies and the private sector, will allow the system to share data intelligence with the right people, enabling them to disrupt scams, live fraudulent activity and cyber breaches.

   Suppliers have submitted their proposals for the new service which CoLP is evaluating. The evaluation will result in a selection of a group of suppliers to take through to the final phases of the procurement. Final suppliers will be chosen before the end of the calendar year.

Outcome 2: People and organisations are prevented from being victims of fraud, and victims are supported (Protect)

CoLP progress MOU with Pension Regulator to help support victims of fraud

2. CoLP’s Victim Care Unit (VCU) and The Pension Regulator (TPR) have now agreed an MOU for the Pension Regulator Contract for Victim Management. This contract has now been signed by both parties. The VCU will work with TPR to coordinate this transition for victims who will receive support by COLP on behalf of TPR. This agreement strongly aligns with our role as National Lead Force and encapsulates the new policing plan Operational Priorities - Protecting the UK from the threat of Economic and Cybercrime and Putting the victim at the heart of everything we do.

Remote Access Scam campaign launched in April 2022

3. Action Fraud has worked alongside City of London Police and TeamViewer to launch a national campaign, to raise awareness of remote access scams. A partner pack containing assets and social media messaging has been circulated, along with the publication of a press release. In 2021, over 20,000 people reported falling victim to scams that involved fraudsters remotely connecting to the victim's computer, with losses totalling over £57m.

Launch of Ticket Fraud campaign in April 2022

4. Action Fraud have launched a national campaign to raise awareness of ticket fraud on Monday. A media pack containing social media assets and messaging has been shared with forces and partners. Welsh assets have been produced to support this activity with key Protect messaging, advice and guidance.

Outcome 3: Police resources are coordinated and deployed efficiently and effectively (Pursue / Protect / Prepare)

City of London Police is responsible for developing and disseminating crime reports for intelligence, protect and pursue action to policing and other law enforcement through the National Fraud Intelligence Bureau. It is also responsible for leading and coordinating the police response to fraud. Its current focus includes increasing judicial outcomes and the effectiveness of operational activity undertaken by policing through leadership and coordination of activity against high harm crimes.

New officers join LFOR under Police Uplift Programme

5. Two police officers joined the Lead Force Operations Room (LFOR) in March under the Police Uplift Programme.

The officers, who will take on the role of Proactive Economic Crime Team (PECT) liaison, will be responsible for co-ordinating activity with the four regional PECT teams. They will offer any support required outside of force areas and offer specialist national lead force resources that could support the new regional teams, which are being established in Yorkshire and Humberside, West Midlands, Eastern and North West.

The PECT teams are at various stages of operational capacity but already some excellent results have been achieved regarding high harm cases disseminated by the national lead force. Examples include positive action regarding a courier fraud linked to a large operation in Wales and a very quick intervention to safeguard a romance fraud victim who lost £150,000.

LFOR has also been updated with some excellent proactive work being conducted outside of lead force tasking and it has been demonstrated how the PECT teams can support national operations such as Operation Henhouse.

The process regarding tasking and co-ordination, investigation tracking and performance monitoring continues to develop and with the additional officers in LFOR, the team are well placed to support the other regions with the development of PECT. In 22/23 we will see regional growth of PECTs in five other regions and London.

LFOR's National Coordination Office continue to engage with forces

6. An interim review of the NLF force engagement plan was conducted following the completion of 17 force visits. This continues to be a significant time and resource effort but manageable with the current skills and capacity and benefiting from excellent feedback. The vast majority of staff/officers visited have been receptive, engaged, see CoLP as assisting and not as a threat – this is due to how the visits have been instigated, arranged, pitched and delivered. Key message from forces is that this interaction is very welcome and will need to be maintained beyond 2022.

   The outputs to date are very comprehensive debrief reports, a series of COT engagements and a list of all the main areas of best practice. The major drivers of this force engagement have been to meet our NLF objectives of coordination and to maintain policing and HO confidence we continue to maximise awareness of the effort, success and achievements through: NLF newsletter, NLF internal communication, Briefing note to all forces on the top 10 areas of best practice

   Success for Operation Henhouse

7. Operation Henhouse, the national fraud intensification campaign, took place throughout March 2022.

   The joint operation between the National Lead Force for Fraud and the National Economic Crime Centre (NECC) had additional funding made available to law enforcement agencies to intensify pursue activity linked to fraud related offences.

   The operation was extremely well received by police forces and regional hubs throughout the UK, with 54 funding applications received. The amount of funding made available exceeded £750,000.

   To date this has resulted in 194 arrests, 13 attempted arrests, 128 voluntary interviews, the issuing of 268 Cease and Desist Notices, and 139 seizures of money and property with a total value of £16,857,816. Operational activity will continue throughout April and public awareness communications are planned once activity has been completed.

National Lead Force courier fraud campaign to be launched

8. City of London Police will be launching its next National Lead Force communications campaign, with a focus on courier fraud, in May 2022.The campaign will run for one week from Monday 16th May to Friday 20th May. Communications materials will be issued to forces approximately two weeks prior to the campaign beginning.

Pre-emptive messaging in response to Ukraine – Russia conflict

9. In response to concerns that fraudsters may seek to capitalise on the conflict in Ukraine, Action Fraud has shared proactive messaging that aims to raise awareness of charity fraud and encourages members of the public to report scam websites, texts and emails. In view of the heightened cyber risk, organisations are being encouraged to bolster their cyber resilience and security via NCSC advice and guidance which has been amplified across Action Fraud channels.

National Lead Force Investigation results in Romance fraud suspect being jailed for 12 months

10. A suspect in a romance fraud case has been jailed for 12 months after a successful collaboration investigation with North Wales Police.

    Having travelled to North Wales to obtain evidence from vulnerable victims, CoLP Officers was able to identify a UK based suspect, through analysis of banking material and communication data.

    Latif Kasule was convicted at Caernarfon Crown Court of seven counts of money laundering and jailed for 12 months.

    Through links forged via the NCA, the investigation team have been able to engage with foreign law enforcement via video conferencing, providing a platform to encourage positive action outside of the UK, targeting perpetrators who cause victims so much emotional and financial harm.

Outcome 4: Fraudsters operating nationally are identified and their offending is being disrupted (Pursue)

City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the

National Economic Crime Centre, as well as stakeholders linked to its funded units.

LFOR helps secure 21 years jail time in large scale courier fraud case

11. The Lead Force Operations Room (LFOR) supported the North East Regional Special Operations Unit (NERSOU) in securing a total of 21 years jail time for an OCG involved in courier fraud.

    City of London Police (CoLP) assisted with Operation Tucson, an investigation looking into the targeting of vulnerable people in the North East and nationwide who fell victim to courier fraud. A total of 16 victims were identified, with losses amounting to over £700,000.

    CoLP assisted with arrests, premises searches and the recovery of evidence which led to a dramatic fall in this crime type in the North East. Following a trial at Durham Crown Court, five offenders were convicted of fraud and money laundering and received significant custodial sentences totalling 21 years. One member of the group received nine years jail time.

DCPCU investigation Op LORUS results in $500,000 crypto seizure

12. DCPCU have recently seized half a million dollars of crypto currency in relation to Operation Lorus. This relates to the arrest and charge of an individual linked to the selling of One Time Password (OTP) software. The OTP software is an online tool for fraudsters. If fraudsters are in possession of compromised banking information the software allows multiple factor authentication to be bypassed. The seizure has gone into a CoLP owned wallet and the investigation continues with a further 10 actors in scope.

Insurance Fraud Enforcement Department increases usage of cease and desist

13. The Insurance Fraud Enforcement Department (IFED) has explored alternative methods of disposal for lower level offenders over the past 18 months, including the use of ‘cease and desist’ notices.

    This method is suitable for cases involving first-time offenders where there is unlikely to be a charge or conviction at court, while still educating the individual and deterring them from committing further criminality.

    After a thorough review of intelligence and a consultation with the party who referred the case, two police officers will attend the offender’s residence to serve the notice. The document outlines the crime which they are believed to be involved in and requests that they ‘cease and desist’ from any future offending, otherwise they may find themselves under criminal investigation.

The individual is then subject to intelligence checks every six months to ensure that they have not reoffended. Out of 48 notices served in the first year of IFED trialling this method, just one individual reoffended.

Outcome 5: Policing has the capability and capacity to detect, disrupt and deter economic crime (Prepare)

City of London Police is a centre of expertise for fraud and is responsible for identifying, developing and disseminating good practice. It provides economic crime investigation training to policing, government and the private sector through its Economic Crime Academy. It is working with policing to build fraud capabilities and reform the fraud operating model.

Fraud and paid-for advertising included in Online Safety Bill

14. Fraud and paid-for advertising will be included in the Online Safety Bill, the Government has announced. City of London Police has been calling for fraud to be included in the scope of the Bill, along with paid-for advertising to stop people from becoming victims of fraudulent online advertisements.

    Last month, the Government announced that fraud would be included as a priority harm within the remit of the Bill and on March 9, it was announced paid-for advertising would also be included within its scope.

    It is estimated that at least 35,000 reports into Action Fraud over the last year were connected to fraudulent online advertising, with victims losing a total of nearly £400,000 as a result. The Online Safety Bill is expected to come before Parliament in the coming months.

The National Economic & Cyber Crime Academy (ECCA) launch new course

15. The National Economic & Cyber Crime Academy has developed a further online course to add to its current offerings. The ‘Demystifying Cyber Enabled Fraud’ course is a great introduction to cybercrime and was designed by an expert team of cybercrime and security trainers. It is suitable for those who do not currently have technical knowledge of this kind of crime and also those who have cyber elements to their role but would like to increase their knowledge. The course complements the Demystifying Cybercrime and Demystifying Blockchain and Crypto packages, but students do not need to have taken those courses in order to engage fully with this one.

    ECCA are also working with Police Now to explore ideas about bringing in new recruits trained to specialise in fraud within their first two years of service.

Cyber Prevention and Disruption Team continue to assist law enforcement with phone and online takedowns

16. City of London Police's Cyber Prevention and Disruption continues to support law enforcement by assisting with phone and online takedowns. The team is part of the National Fraud Intelligence Bureau (NFIB) and is made up of five detectives who are dedicated to identifying and disrupting the key enablers used in fraud, namely UK registered phone numbers, emails, websites and social media accounts.

    Last year, the team disrupted over 1,100 websites actively involved in fraud, with a further 8,500 websites created for fraud disrupted before they went live. Over 600 emails and 400 phone numbers used in fraud were also taken down, all of which were calculated to have resulted in losses of over £144 million.

National Romance Fraud Toolkit launched by CoLP

17. Following a successful Romance Fraud investigation by City of London Police, a Romance fraud Toolkit has been developed and rolled out nationally, utilising the learning and experience gained from this investigation. The toolkit has been created in order to assist investigating officers investigating this crime type and to help disrupt and detect Romance fraudsters.

Intellectual Property Office launch new counter-infringing strategy

18. The IPO launched its intellectual property counter-infringing strategy 2022- 2027 in February, with the key document outlining new process and highlighting new and emerging trends. PIPCU works closely with the IPO to assure its enforcement actions are in line with the overarching strategy and supports the goals of the IPO in protecting the UK from the negative economic impact of this type of criminality

CONCLUSION

19. This report provides an overview of the NLF outcomes and highlights a selection of activities being delivered in pursuit of these outcomes.

Committee: Economic and Cyber Crime Committee	**Dated:** 13 May 2022
Subject: Cyber Griffin Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	**N/A**
Does this proposal require extra revenue and/or capital spending?	**NA**
If so, how much?	**N/A**
What is the source of Funding?	**N/A**
Has this Funding Source been agreed with the Chamberlain's Department?	**N/A**
Report of: Commissioner of Police Pol 24-22	**For information**
Report author: DS Charlie Morrison, Cyber Griffin Team	

SUMMARY

Cyber Griffin had a strong start to the year but will experience a temporary levelling-off of service delivery in the next quarter as the unit enters a challenging period due to resourcing wider policing demands. The programme has received twelve months of additional funding and within that an agreement to hire an Inspector as well as two additional Constables. The intention now is to use this additional resource to bolster the team's resilience as demand increases and to pilot several opportunities which will provide a greater level of service. These include a new security deliverable, work which contributes to a greater national role and exploration of potential overseas opportunities. Case study evidence of these pilots will be provided and used as the basis upon which future decisions about direction can be made. The programme's duty to provide security advice and guidance within the Square Mile will remain its priority and resourcing will be closely monitored to ensure this objective is met.

RECOMMENDATIONS

It is recommended that Members note the report

MAIN REPORT

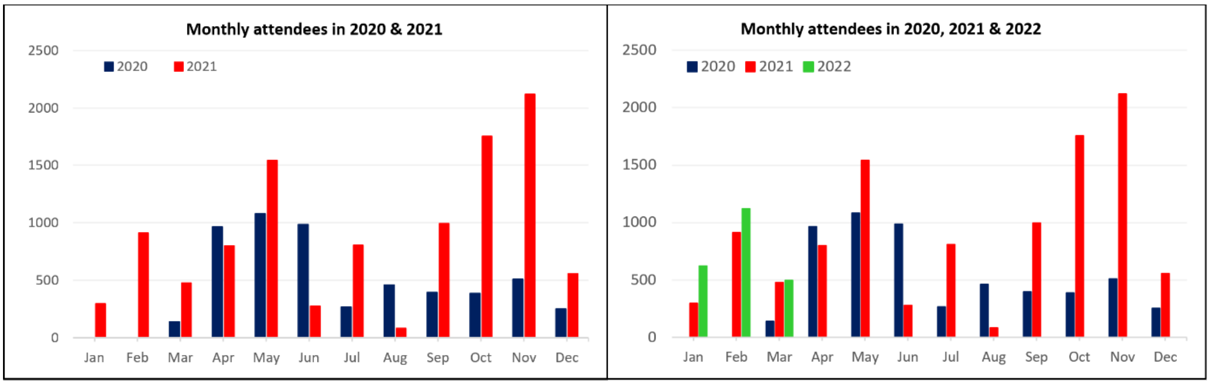
INTRODUCTION

1. This report will give a brief update on the current position of the Cyber Griffin programme. For details of Cyber Griffin deliverables please visit: www.cybergriffin.police.uk

CURRENT POSITION

2. Cyber Griffin had achieved record service delivery levels in the last quarter compared with previous years. The digital platform used by programme remains an excellent means of scaling services to meet demand and a useful tool for providing resilience when the unit has to operate on limited numbers. Demand for physical deliveries, which currently make up approximately 15% of total engagements, remains low but has risen very slightly. The programme has maintained an approximate two month lead time for service delivery. The team maintains the resilience required to manage victims and urgent calls for service. Priority matters are met within the timeframes set by national standards.

Tables Showing Cyber Griffin's monthly attendees compared with previous years



3. Regarding locally set targets, Cyber Griffin's performance has been largely positive. Cyber Griffin regularly exceeds the number of people engaged when compared with the same month in previous years (please see Cyber Griffin monthly attendee's graphs above). This is a positive indication that the programme continues to grow year on year. Cyber Griffin also achieved its annual local targets for the calendar last year. These were to train 7,000 people (number trained 10,392), to deliver 150 services (number delivered 268) and to engage with 100 new businesses (number of new businesses engaged 180). Please note two important changes to future reporting. Firstly, Cyber Griffin will be moving from calendar year reporting to financial year reporting. Secondly, the programme has been set more ambitious performance targets for the coming financial year. These will be set out in the next quarters performance reporting.

4. Regarding performance against national targets, Cyber Griffin continues to meet all nationally set key performance indicates (KPIs). Specifically, the programme has engaged with 100% of victims of cyber-dependent crime within its force area and survey data demonstrates that engagements create security behaviour changes in above 75% of attendees. The same events have a satisfaction rate of above 75%.

5. Looking ahead at performance, Cyber Griffin is forecast to go through a challenging quarter as the unit experiences the impact of having resourced wider policing demands. It is expected that delivery will temporally dip and that the

programme will have to recover this lost ground later in the year. The current expectation is that this shortfall can be recovered. Of particular note is a sharp fall in new businesses engaged with. This does not show on reporting currently but will appear in the next quarters return. Officers have already been briefed on this issue and will be re-focused on new business engagement.

6. Cyber Griffin's short-term financial situation is very positive. The team have just recruited an Inspector and are in the process of recruiting two additional Constables. The team are well provisioned with equipment and have retained the current staff, meaning that the new joiners will be supported by experienced and fully trained colleagues. Funding will again become a focus as the force approaches the 2023/24 financial year.

7. In addition to delivering the programme's core services, Cyber Griffin aims to explore a number of pilot projects in the coming months. These include; launching new services within the Square Mile, delivering briefings on a national level and conducting work overseas, all with the potential to reduce Cyber Griffin's running costs whilst also strengthening and extending the unit's brand. A case study of each pilot will be completed and used as the basis on which to decide Cyber Griffin's direction in future years. This year marks an excellent opportunity to explore and document what the programme is capable of delivering.

8. Cyber Griffin continues to work with Bristol University in the development of a new Incident Response Exercise. The exercise algorithm is close to completion after an initial round of testing and is expected to enter a phase of exercising with real participants in the coming two months. What separates this training from alternatives is that Cyber Griffin will be offering an 'open world' exercise. This means that participants will be able to use the exercise multiple times to sharpen their incident response skills as the algorithm will randomly generate scenarios from a pool of hundreds of possible scenarios the team have developed over the last three years. This marks a significant progression from traditional more linear 'paper-feed' exercising.

CONCLUSION

9. Cyber Griffin have experienced a strong start to the year but will go through a weaker period of service delivery as the unit resources wider policing demands. Overall, the programme should recover to meet the targets set both locally and national. Funding has enabled the unit to recruit additional officers. This will increase the unit's capability and enable Cyber Griffin to explore new service offerings both in and outside of the Square Mile. Analysis of these pilots will inform how the programme can be best utilised in the longer term.

This page is intentionally left blank

National Lead Force Performance Report

Q4: January – March 2022

Agenda Item 8

Performance Assessment - Key:

The dashboard provides an assessment of City of London Police performance against the National Lead Force (NLF) aims and objectives as set out in the National Lead Force Plan 2020-2022 (NLF Plan).

The NLF Plan was approved by the City of London Police Authority in October 2020. The plan sets out how City of London Police will improve the national response to fraud. It reflects NLF's contribution and commitment to the National Fraud Policing Strategy and the National Economic Crime Centre's (NECC) five-year strategy. The NECC leads the 'whole system' to drive down the growth in fraud on behalf of the UK Government.

The NLF plan sets out five outcomes that City of London Police is seeking to achieve: -

Outcome 1 - The public has confidence in the Action Fraud reporting service
Outcome 2 - People and organisations are prevented from being victims of fraud, and victims are supported (National Fraud Policing Strategy)
Outcome 3 - Police resources are deployed efficiently and effectively against fraud threats (National Fraud Policing Strategy)
Outcome 4 - Fraudsters operating nationally are identified and offending is disrupted
Outcome 5 - Policing has the capability and capacity to detect, disrupt and deter perpetrators of fraud (National Fraud Policing Strategy)

In order to identify if these outcomes are being achieved a series of success measures for each outcome have been produced and are reported on throughout this period. The success measures related to each outcome can be found at the start of each slide alongside the current RAG assessment for the relevant success measures.

The below chart identifies the RAG assessment criteria for the success measures.

Table 1 – Success Measure Performance RAG assessment

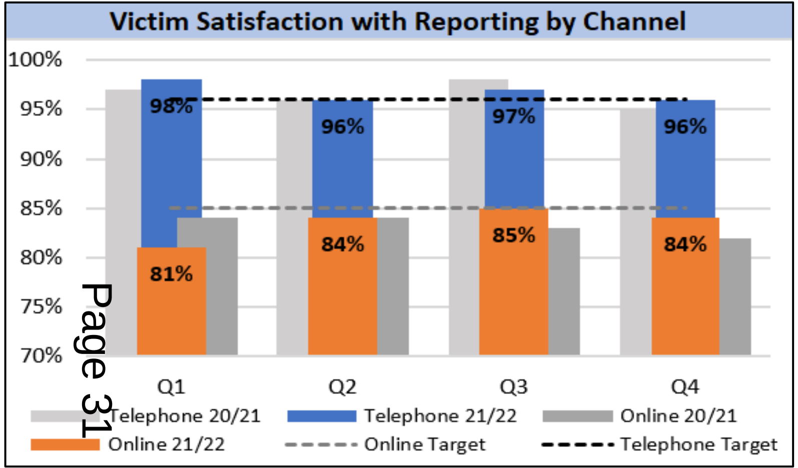
Green	The success measures are being met
Amber Green ▨	The success measures have not been consistently met but there is sufficient evidence to show that developments are being made to improve the RAG status of the measures to green by the end of the period
Amber Red ▨	The success measures have not been consistently met and there is insufficient evidence to show that developments are being made to improve the RAG status of the measures to green by the end of the period
Red	It is unlikely the success measure will be met for the annual period based on the success shown in quarters to date
Grey	Insufficient evidence means that no meaningful assessment is possible at this time.

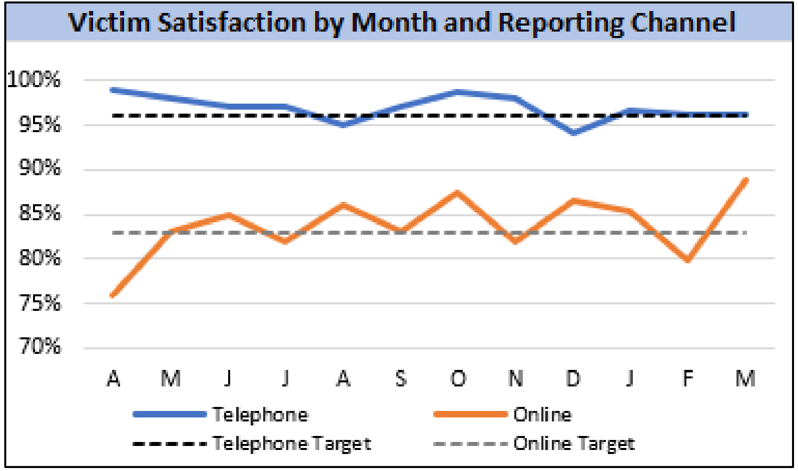
Outcome 1: *The public has confidence in the Action Fraud reporting service.*

NLF Role: City of London Police operates the national fraud and cybercrime reporting service. Responsibilities include providing a first point of contact for victims of fraud, crime reporting and triage.

Success Measures:

- **96% of survey respondents are satisfied with the telephone reporting service.** **GREEN**
- **85% of survey respondents are satisfied with the online reporting service.** **AMBER**


Victim Satisfaction with Reporting by Channel


Victim Satisfaction by Month and Reporting Channel

The main Action Fraud satisfaction survey indicates that satisfaction with the telephone reporting service remains consistent and on target at 96% for the quarter. The overall satisfaction for the year is 97%, exceeding the target.

Satisfaction with online reporting has fluctuated during the period, reaching a high of 89% in March, only dropping below the target to 80% in February. At 84%, satisfaction for the quarter fell just short of our target of 85%. Satisfaction for the 2021/22 financial year also fell just short of our target at 84%. Overall, online satisfaction has seen a marked improvement since the introduction of the virtual advisor 'chatbot' service in May, in addition to improved signposting on the website.

Since the launch of the current victim satisfaction survey, Action Fraud advisors have provided a consistently good service. Overall, 1% of those reporting a crime in Q4 opted to provide satisfaction feedback to the confirmation fulfilment survey. Over 1.39M confirmation survey links have been delivered to date, with 15,982 respondents opting to provide satisfaction feedback, including free text responses which are used to continuously improve our service.

The number of Action Fraud complaints logged in Q4 2021/22 increased by 131% from 84 in Q3 to 194. During the quarter, 155 cases have been finalised as either resolved or it was found that the service was acceptable.

The most commonly received complaint was in the category A2 – Decisions, often due to the non-investigation of a report.

Outcome 1: *The public has confidence in the Action Fraud reporting service.*

NLF Role: City of London Police operates the national fraud and cybercrime reporting service. Responsibilities include providing a first point of contact for victims of fraud, crime reporting and triage.

Success Measures:

- Average time taken to answer within Action Fraud is 5 minutes* 🟥
- The percentage of reports to Action Fraud that are abandoned is below 16%* 🟥

* These benchmarks are based on an assumed static demand level from 2019/20.

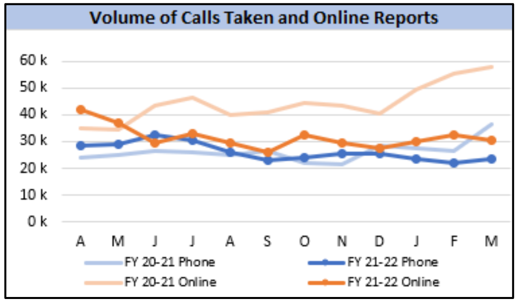
The number of calls answered by Action Fraud fell by 8% from 74,906 in Q3 to 68,933. This represents a reduction from the same quarter in the previous year (90,164) and an increase on Q4 2019/20 (61,749). Last year saw the highest ever volumes into the service in one quarter, but demand has now returned to expected volumes resulting in subsequent reductions in calls handled and reports submitted.

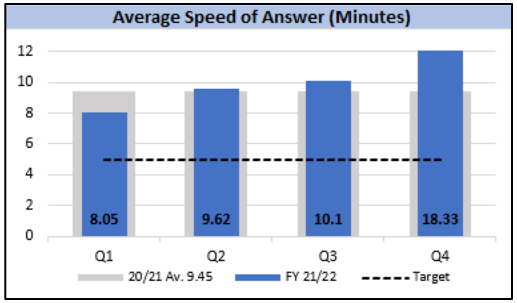
Volumes of online reports received rose slightly this quarter, from 89,810 in Q3 to 93,232 in Q4. This represents a small decrease of 6% from Q1 when levels were at their highest. Some of this decrease is due to seasonality.

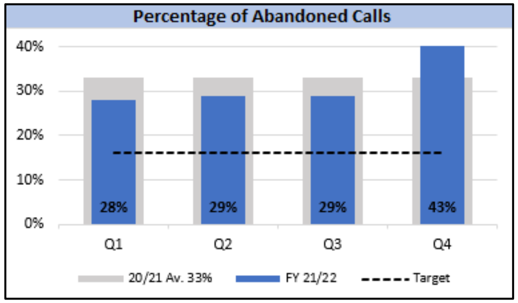
The average time taken to answer calls in Q4 was 18.33 minutes which is slower than the previous quarters this year and nearly double the monthly average of 9.45 minutes from 2020/21. March showed some recovery at 18 minutes from the February peak of 21, the target of answering calls within 5 minutes was not met in any month this year.

Call abandonment figures increased quarter on quarter to 43% and sit below the financial year average of 33.8%. Again February saw the highest call abandonment figures, but the whole quarter remained above 40%. The target of 16% was not met this year.

Q4 performance was impacted by staffing challenges including vetting delays, onboarding of new starters, attrition, high covid absence and annual leave. Storm weather and outages in the reporting system also impacted the service across a total of 6 days in February, resulting in manual reports being taken on two separate occasions.







Quarter 4 was challenging in the Contact Centre, with system outages and power issues connected to Storm Eunice both having a negative affect on performance. There were also staffing shortages due to covid related sickness and annual leave. Measures have been put in place to mitigate these in the coming months.

Staff turnover is also still a factor, with more call handlers leaving than joining due to vetting issues. A plan is in place to recruit internal candidates who can be processed quicker, and effort has been put into upskilling the existing workforce while awaiting new starters.

On the online reporting tool, the Chatbot development has continued and all guests who aim to chat, now come through the menu provided. Phase 2 of the project is now live, and provides 60+ informational and guidance responses via a neural language bot, to free text questions from service users. This has resulted in further capacity to support the inbound voice service and uptake is now stable.

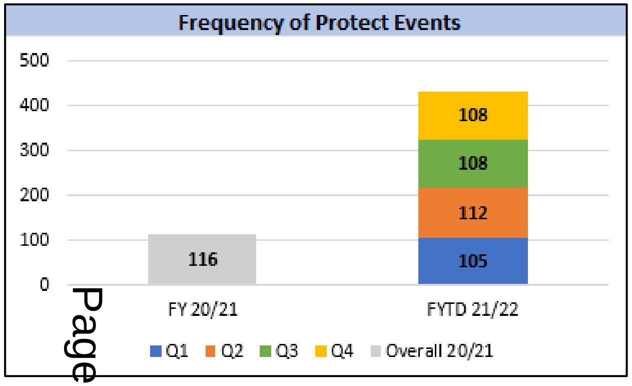
Outcome 2: *People & organisations are prevented from being victims of fraud, & victims are supported.*

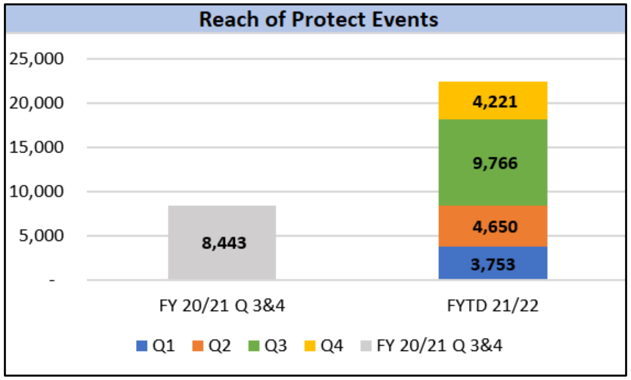
NLF Role: City of London Police is responsible for providing first contact support for victims who report to Action Fraud. It is also responsible for developing and disseminating national protect messaging for policing based upon latest crime reporting trends.

Success Measures:

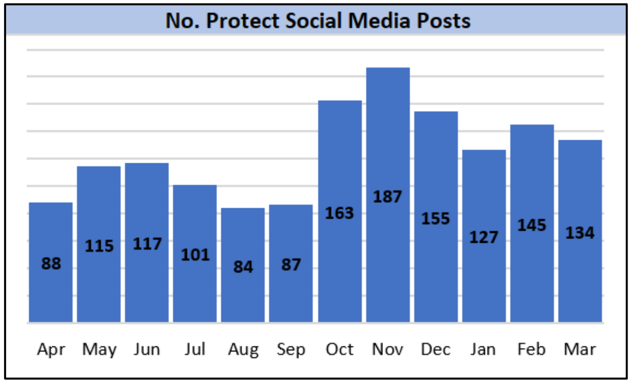
• Maintain the reach of protect messaging*	🟩
• Establish a baseline for use of protect messages through CoLP online and offline media channels and engagement events.	🟩

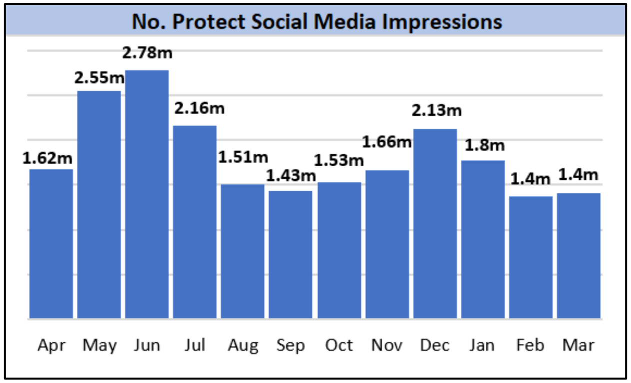
*Stretch Metric – Extend the reach of Protect messaging by 10%


Frequency of Protect Events


Reach of Protect Events

The force continues to develop its understanding of engagement and reach for protect messaging; in order to establish the relevant baseline through online and offline media channels. There are processes in place to collect data for the number of Protect events and social media posts each quarter, and to record the numbers of attendees and impressions linked to these. Next steps will involve engaging with attendees to understand the effectiveness of the content and whether behaviour will change, and the reach of social media posts. Impressions are defined as the number of people your content is visible to, while reach refers to the number of people engaging with your content through likes, comments and shares.


No. Protect Social Media Posts


No. Protect Social Media Impressions

The number of protect events were significantly lower in 2020/21 than previous years; as restrictions were imposed due to Covid-19. However, teams found new ways of engaging with stakeholders and the public, in particular using online events which can reach greater numbers. This recovery continued in Q4 of this year, with 4,221 people attending 108 events. Of particular note, over 2,000 people attended online events held by DCPCU in March.

Following the increased activity relating to Black Friday and Christmas related frauds in Q3, Action Fraud social media output remained high compared to the first half of the year. The top engagements related to various phishing scams.

Across the quarter, the Media Team oversaw 12 press releases and 8 interviews, including an interview about ‘cash for crash’ with BBC’s Crimewatch. Subject matter included the annual Valentines romance fraud awareness campaign and IFED’s 10 year anniversary.

The NFIB released 6 alerts through its digital community messaging platforms. These platforms reach approximately 600,000 users each time an alert is sent.

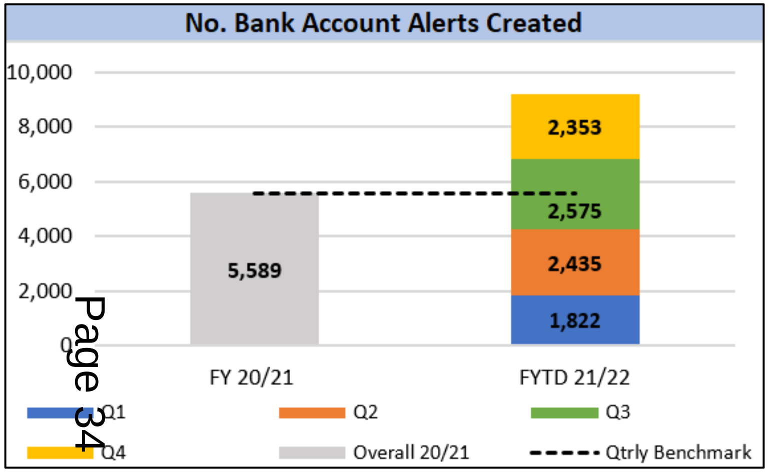
Outcome 2: *People & organisations are prevented from being victims of fraud, & victims are supported.*

NLF Role: City of London Police is responsible for providing first contact support for victims who report to Action Fraud. This includes the banking sector, utilising initiatives to identify and disrupt accounts used in Payment Fraud.

Success Measures:

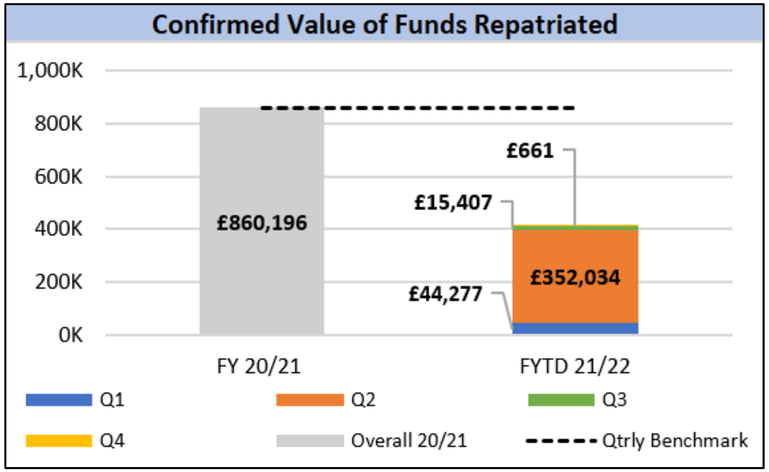
- The value of transactions confirmed as prevented or disrupted before passing into criminal hands is increased* 🟥

*The ambition is to increase this by 25% of 20/21 funds for the year with a stretch metric of a 50% increase.



CoLP is continuing its long standing initiative to alert banks to accounts used in fraud. The monthly average of referrals has steadily increased from 164 alerts in 2019/20 and 466 in 2020/21, to 765 for 2021/22. January recorded a peak of 950 alerts sent to banks, followed by slightly lower numbers in February and March. The confirmed value of repatriated funds is reliant on feedback from banks which is not always available. The confirmed average monthly savings rose sharply from £14,759 in Q1 to £117,345 in Q2, but then fell to only £1,548 in Q3 and £661 in Q4. This is partly due to a £173,000 payment diversion fraud repatriated in July. For the financial year to date CoLP have alerted banks of accounts used to receive the proceeds of fraud to the amount of £35,124,518 and as a result £412,379 has been confirmed as recovered since April.

The number of disrupted bank accounts has been rising since the inception of the project and the initiative allows not only for funds to be returned to victims, but also disrupts fraudsters, demonstrates good partnership working, and provides CoLP with the ability to start an investigation early if an alert is missed by the banks. A solution regarding automation of early reporting back to banks in a more consistent and timely manner went live in May. The system is not linked to UK Finance systems at this time, so feedback will continue to rely on manual reporting from banks until this is resolved.



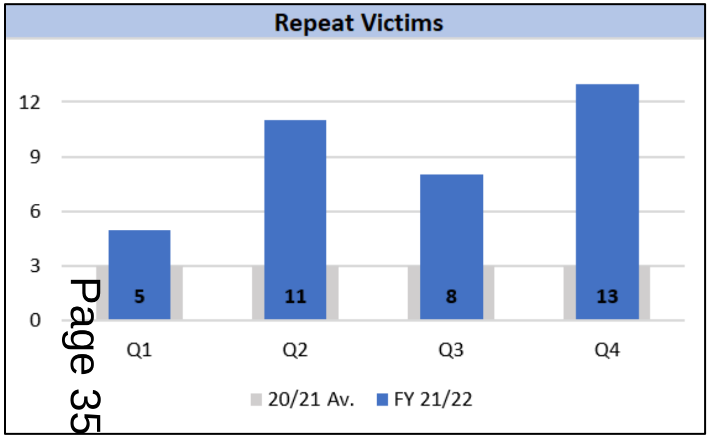
Additional funding has been received through the Lloyds collaboration to further automate alerts into the UK Finance BPS system; which many banks are using to identify monies at risk across industry. The additional benefit of this work, is to also automate the feedback from the banking industry back into CoLP as to the outcomes of the alerts sent by NFIB. The aim is to enhance feedback on action taken and funds repatriated to victims whilst reducing the manual effort to both chase, and send an outcome back to CoLP. Work is ongoing as to the feasibility of this solution working with UKF, CoLP IT and IMS with a delivery date on or before August 2022. In the meantime efforts have been made to improve the current process with individual banks utilising a CoLP volunteer working in the financial industry; to increase reporting of outcomes back into the NFIB.

Outcome 2: *People & organisations are prevented from being victims of fraud, & victims are supported.*

NLF Role: City of London Police is responsible for providing first contact support for victims who report to Action Fraud . It is also responsible for developing and disseminating national protect messaging for policing based upon latest crime reporting trends.

Success Measures:

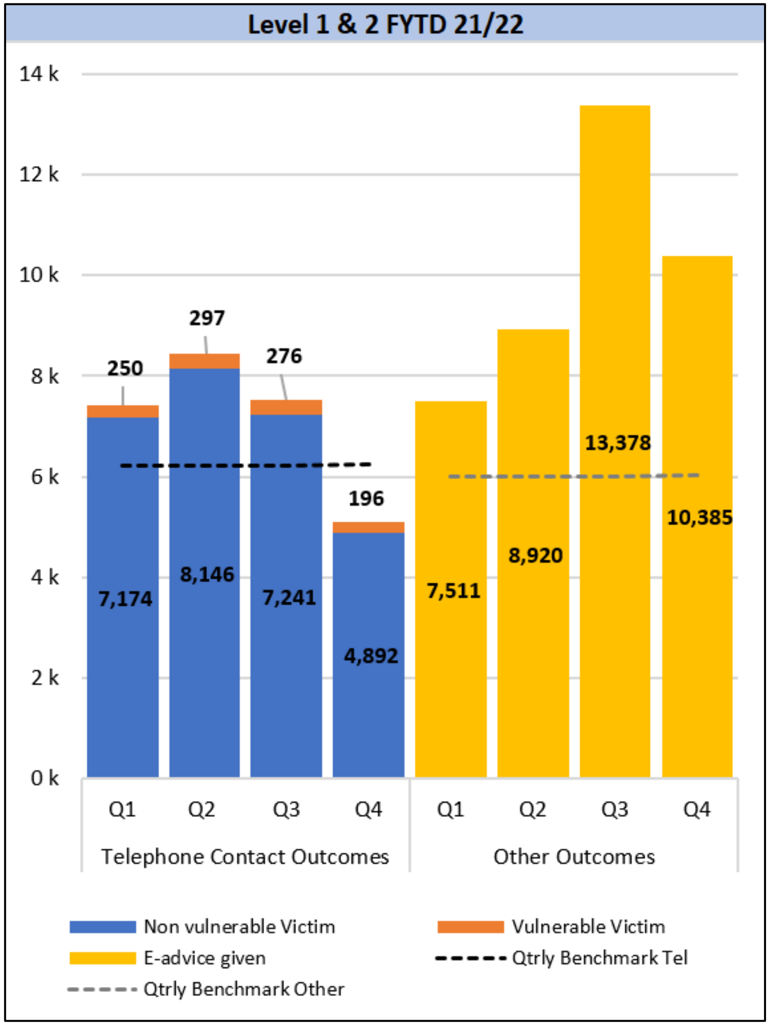
• The Economic Crime Victim Care Unit will maintain the level of support provided to victims	🟩
• The Economic Crime Victim Care Unit will sustain the low levels of repeat victimisation following interaction with their service	🟩



During the period, 13 repeat victims were recorded. Despite this being an increase on the 12 repeat victims recorded in 2020/21, as this is only 0.05% of total victims engaged with, levels of repeat victimisation remain low.

The National Economic Crime Victim Care Unit (NECVCU) supports forces at a local level, delivering care to victims of fraud and cyber-crime, allowing for a consistent and national standard of care and support. The **Level 1** service gives Protect/Prevent advice to non-vulnerable victims of fraud. The **Level 2** service engages with victims when vulnerability is identified, and by giving crime prevention advice and signposting to local support services helps the victim to cope and recover from the fraud. Six forces are currently covered by both Level 1 and 2 services, with a further 14 receiving Level 1 only. The NECVCU is looking at onboarding more forces and have conducted 19 trials.

In the fourth quarter of 2021/22 the NECVCU has performed above 2020/21 averages with the volume of e-advice given, but the numbers of telephone contacts fell for the Level 1 service in March due to vetting issues, while remaining stable for Level 2. During the period, NECVCU has engaged with 17,934 victims. Between January and March 2022, 9 victims have requested additional advice over suspicious emails or phone calls, preventing re-victimisation and an estimated £145k in fraud. 77 victims have been provided with additional safeguarding support. Over the past 12-18 months NECVCU have supported victims to recover over £1,220,000.



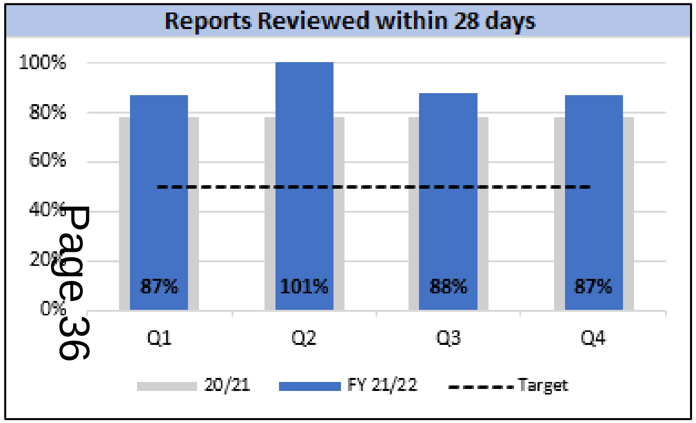
Outcome 3: *Police resources are coordinated and deployed efficiently and effectively.*

NLF Role: City of London Police is responsible for developing and disseminating crime reports for intelligence, protect and pursue action to policing and other law enforcement through the National Fraud Intelligence Bureau. It is also responsible for leading and coordinating the police response to fraud.

Success Measures:

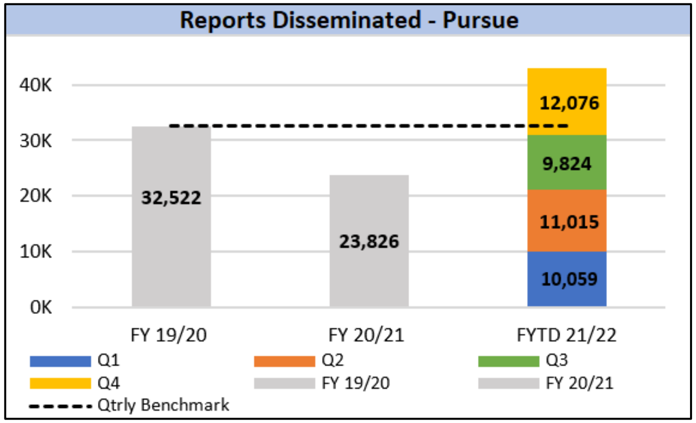
- 50% of crimes that meet the threshold are reviewed within 28 days 🟩
- The number of crimes disseminated for investigation is increased* 🟩

* The ambition is to sustain 2019/20 levels as per graph benchmark.



All fraud reports received are triaged against agreed thresholds and prioritised for review. The highest harm frauds are prioritised and the reports are further examined. Levels of harm are set each year through a MoRiLE process where each fraud and cyber crime type is ranked and the highest ranked for potential harm and risk become priority control strategy crimes. Once the report is reviewed a decision will be made about the viability of cases and most appropriate agency to investigate them. The report will then be disseminated to that agency. If the report is not reviewed or disseminated then Protect Advice is sent to the victim and they may be referred to the National Economic Crime Victim Care Unit if appropriate.

Due to technical issues the data for triaging times was unavailable for some time. We now have preliminary figures from project DROID and are awaiting final sign-off of these, figures could be subject to change in future reports. Current indications are that throughout the year 91% of reports that meet the threshold for investigation have been reviewed within the 28 day target.



A total of 12,076 Pursue reports were disseminated in Q4, the highest quarterly volume of the year, and bringing the total Pursue reports disseminated to 42,974, a 32% increase from the 2019/20 benchmark. (Note: this excludes reports that are disseminated for intelligence purposes or victim care). There is work ongoing to link in with Action Fraud and improve the quality of the fraud reports taken. For example, the use of mandatory fields for vital information such as bank account details will reduce the volume of additional enquiries made during initial investigations; and streamline the review and dissemination processes.

The dissemination of Control Strategy crimes also surpassed the 2020/21 quarterly average of 2,553, with 3,235 crimes sent this quarter. Control Strategy priority crimes include: Romance Fraud, Courier Fraud, Investment Fraud, Payment Diversion Fraud, Insurance Fraud and Banking/Payments Fraud. This is in line with the campaigns run throughout the year, focusing on a number of these areas along with COVID-19 related fraud.

Outcome 3: *Police resources are coordinated and deployed efficiently and effectively.*

NLF Role: City of London Police is responsible for developing and disseminating crime reports for intelligence, protect and pursue action to policing and other law enforcement through the National Fraud Intelligence Bureau. It is also responsible for leading and coordinating the police response to fraud.

Success Measures:

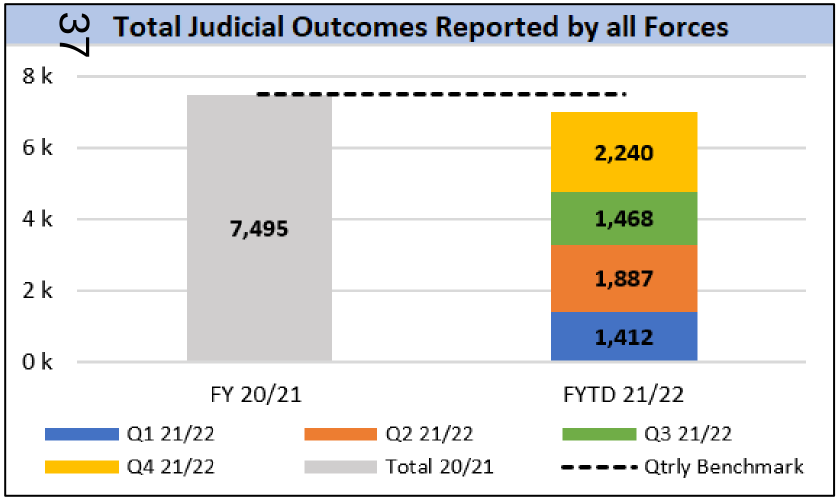
- The number of judicial outcomes recorded by policing is increased. 🟥
- 100% of Home Office forces are in the compliant category for outcome reporting. 🟩

Forces are required to provide outcome information to CoLP every month, matched against their NFIB disseminations. In Q4, all forces continued to provide a return each month. The National Coordinators continue to engage with forces to ensure this 100% compliance can be maintained throughout the year.

FY 20/21	Returns
Compliant (10-12 Returns)	39
Partially Compliant (7-9 Returns)	3
Non Compliant (0-6 Returns)	3

FY 21/22 FYTD	Returns
Compliant (10-12 Returns)	45
Partially Compliant (7-9 Returns)	0
Non Compliant (0-6 Returns)	0

Total Judicial Outcomes Reported by all Forces



The number of judicial outcomes reported nationally in Q4 peaked at 2,240 bringing the total to 7,007 for the year. This is a 7% deduction from the previous year's total outcomes. Non-judicial outcomes also fell slightly, from 57,826 in 20/21 to 57,424 in 21/22.

The total outcomes reported in the period can relate to disseminations from any time frame. The volume of outcomes fluctuates throughout the year as, for example, one investigation into a boiler room might have hundreds of outcomes attached to it.

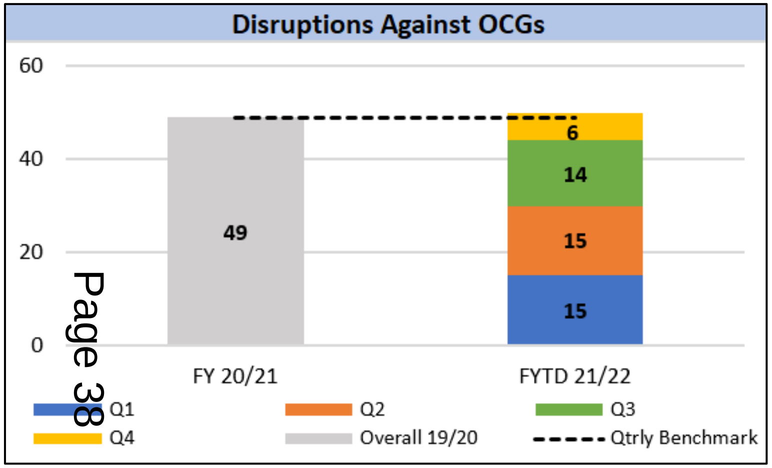
When considered in relation to the number of crime report disseminations that have been made during FY 2021/22, this gives a judicial outcome rate of 25%.

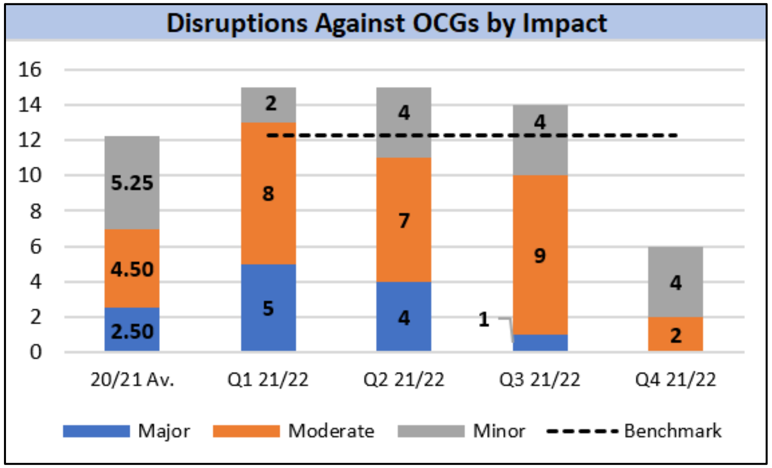
Note: Judicial outcomes refer to Home Office Counting Rules Outcomes 1-8 which include charges, cautions, taken into consideration etc (they do not refer to the wider criminal justice process).

Outcome 4: *Fraudsters operating nationally are identified and their offending is being disrupted.*

NLF Role: City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the National Economic Crime Centre, as well as stakeholders linked to it's funded units.

Success Measures:	
• CoLP OCG disruptions are sustained with higher proportion of major disruptions.	🟩





There are currently 65 mapped Organised Crime Groups (OCGs) under investigation by National Lead Force teams. Eight new OCGs were mapped in Q4 and four were closed.

There were a total of 6 disruptions during Q4 2021/22, which is half the quarterly average of 12 from the previous year. However, this exceeds the number of disruptions recorded for Q4 of 2020/21 (4) suggesting a possible seasonal variance in Q4.

Although no major disruptions were recorded in Q4, the total for the year is 10, which is the same as 20/21 and slightly less than 19/20. Overall, the number of disruptions has increased by 1, with the greatest proportion being of moderate impact.

- Two moderate disruptions were claimed in Q4 relating to the arrest of a key nominal and seizure of digital devices in a Fraud Team case, and two subjects pleading guilty to producing counterfeit Bio Oil in a PIPCU investigation.
- The moderate disruptions included the arrest of a professional enabler, and warrants, seizures and intelligence gathering conducted against a number of key nominals in cases across the NLF teams.
- The City SOC team continue to receive and assess NLF referrals where appropriate for proactive support and investigation.

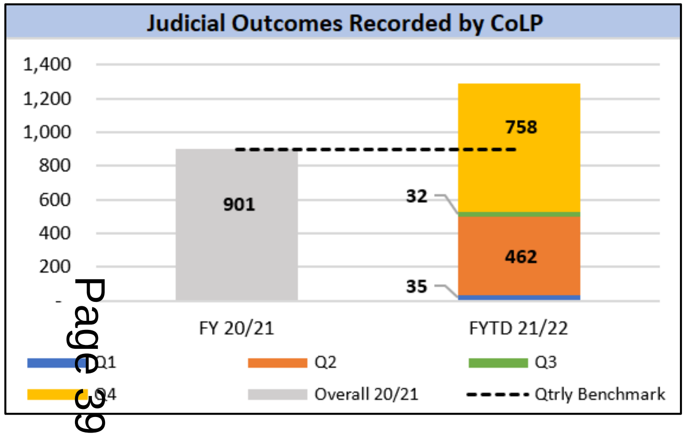
Outcome 4: *Fraudsters operating nationally are identified and their offending is being disrupted.*

NLF Role: City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the National Economic Crime Centre, as well as stakeholders linked to it's funded units.

Success Measures:

Increase the number of judicial outcomes recorded by City of London Police.*	🟩

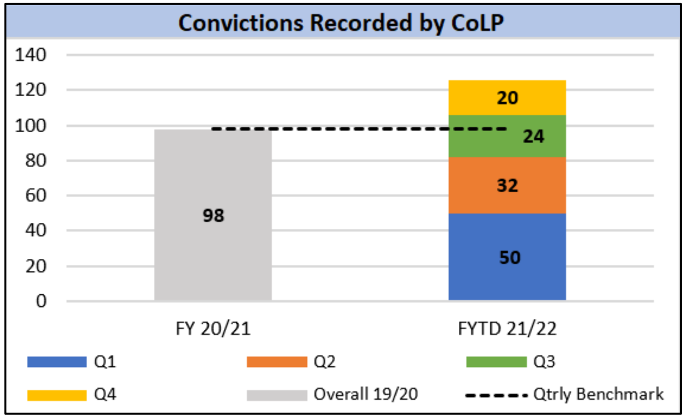
*The ambition is to increase by 25% with a stretch metric of 50% of 20/21 outcomes



Pursue activity was affected by the pandemic throughout the previous year, with lower numbers of arrests, interviews, cautions and charges than in 2019/20. Each quarter of 2021/22 has seen recovery of activity levels across all of these measures, reaching a peak in March with officers reporting 24 arrests and 34 interviews under caution.

The chart to the left shows that following the high numbers of judicial outcomes reported in 2020/21 and Q2, the numbers dropped considerably in Q3 of this year, before rising again in Q4. The 2021/22 total of 1,287 judicial outcomes represents a 43% increase from the previous year.

A significantly higher number of judicial outcomes were recorded by CoLP in Q2 and Q4, with outcomes posted for a number of notable operations, each giving multiple outcomes and some providing closure for hundreds of victims. This fluctuation is expected as cases with varying numbers of crimes attached are seen in courts throughout the year.



In Quarter 4, there were less convictions for cases that had been tried during the current reporting period than in previous quarters. However, the Q4 total of 20 convictions brings the overall number for 2021/22 to 126, surpassing the annual count from 2020/21 and showing a return to pre-pandemic levels.

Notable successes throughout Q4 included a fraud by false representation where the suspects defrauded a hotel of £125k; one suspect was recently extradited from the US and convicted. Another conviction was obtained where two fraudsters had colluded to obtain mortgages using fraudulent information resulting in tens of thousands of pounds. A previous trial had to be abandoned at a late stage as several jury members contracted COVID-19. A high profile suspect was found guilty for fraud by false representation by claiming on an alleged collision at a time when no motor insurance policy existed.

Note: Judicial outcomes refer to Home Office Counting Rule Outcomes 1-8 which include charges, cautions, taken into consideration etc, they do not refer to the wider criminal justice process.

Outcome 4: *Fraudsters operating nationally are identified and their offending is being disrupted.*

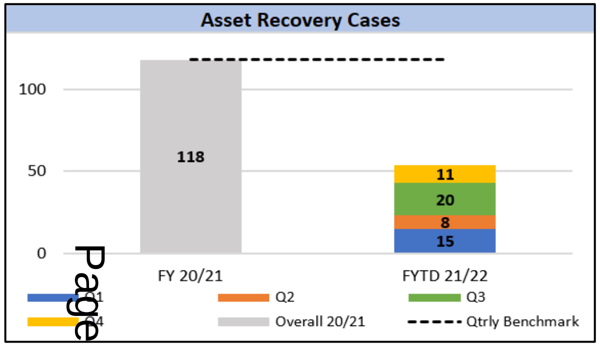
NLF Role: City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the National Economic Crime Centre, as well as stakeholders linked to it's funded units.

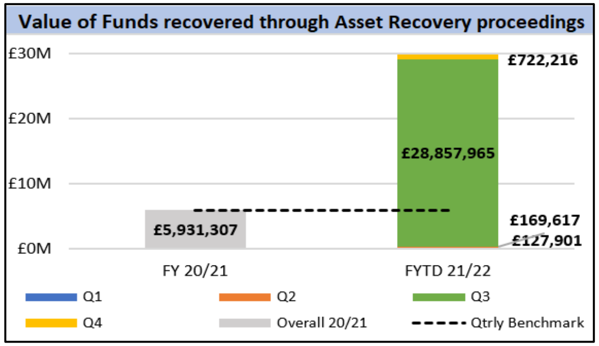
Success Measures:

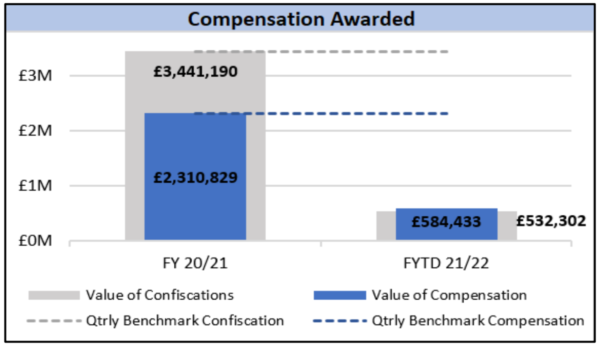
- Increase use of POCA powers and value of assets denied.[2] ▨
- Increased use and number of new ancillary orders issued by City of London Police.[3] 🟩

[2] ambition is to increase by 5% with a stretch metric of 10% of 20/21 occasions.

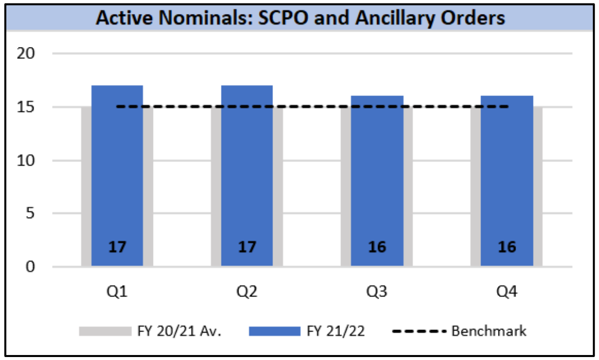
[3] ambition is to increase by 30% with a stretch metric of 60% of 20/21 occasions.

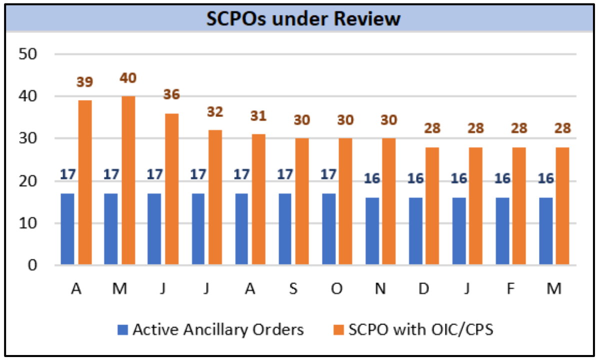






There has been an overall 54% drop in POCA activities compared to the previous year. Throughout the Financial Year, the value of these orders has reduced considerably across all measures with the exception of Account Forfeiture, when in Q3 the Asset Recovery Team working in partnership with the CPS obtained two Account Forfeiture orders totalling over £28.75m; the UK's highest ever account forfeiture. Then, as an offshoot to this ground breaking investigation, an Account Freezing Order was obtained for £1.48m. Decreases in POCA activity are being seen nationally and the Strategic Asset Recovery Board is investigating this change.
Responding to these changes in POCA activity, officers have sought innovate ways to compensate victims. In one case, officers attended court under the Police Property Act and obtained an order for a Rolex valued at £36k seized during the investigation be delivered to an elderly victim of courier fraud.





The active ancillary orders include Serious Crime Prevention Orders, Financial Reporting Orders and Criminal Behaviour Orders.

Throughout the year numbers fluctuate as orders expired and new ones have been served. Quarter 4 has remained at 16 active Ancillary Orders, 1 above the 20/21 benchmark.

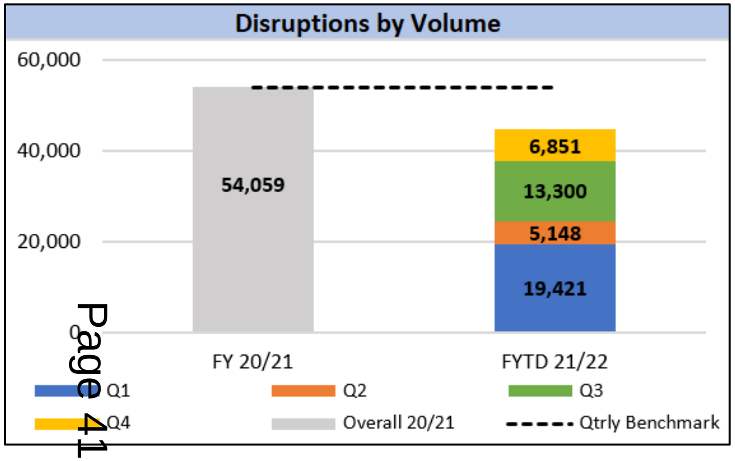
Currently CoLP have 28 SCPOs under review with OIC/CPS and 16 Active Ancillary Orders with one order having expired in September.

Outcome 4: *Fraudsters operating nationally are identified and their offending is being disrupted.*

NLF Role: City of London Police investigates nationally significant, serious and complex fraud on behalf of policing. It received referrals from a range of stakeholders including police forces, ROCUs, National Fraud Intelligence Bureau and the National Economic Crime Centre, as well as stakeholders linked to it's funded units.

Success Measures:

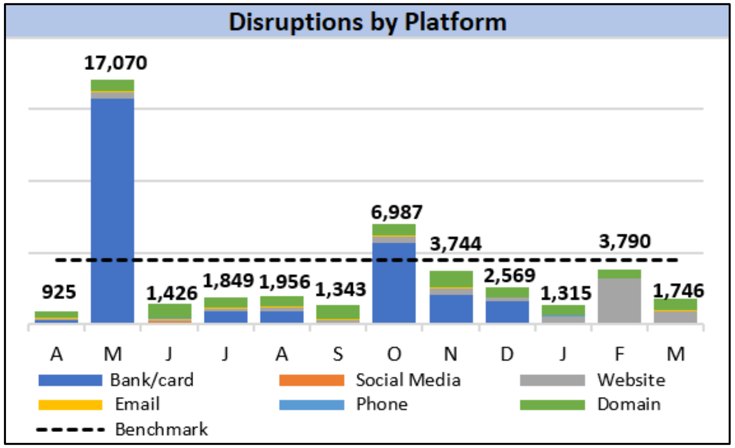
- The number of disruptions to technological enablers is sustained. 🟥



Disruptions by Volume

During Quarter 4, 6,851 disruptions were recorded; this takes the total for the year to 44,720, a 17% reduction on the 2020/21 final figure. Although performance in disruptions was consistent across all measures during 2021/22, the previous year saw a number of focused operations, particularly around bank cards, which only took place during May 2021 in this period.

During the forth quarter, there was a particular intensification in website disruptions by both the NFIB Prevention and Disruption Team (P&D), and the PIPCU operation to disrupt fraudulent domains. Activity in this area during Q4 accounted for over half of the annual total, with teams accepting referrals of single fraudulent websites and identifying multiple others created by the same registrants.



Disruptions by Platform

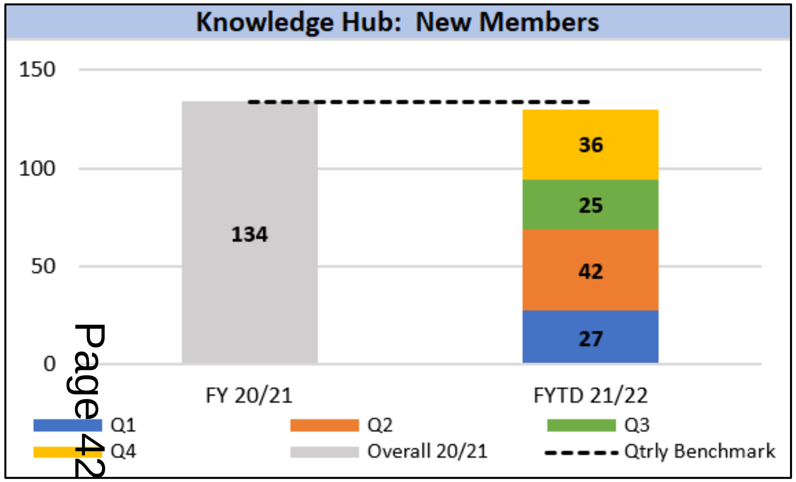
City of London Police and National Cyber Security Centre Suspicious Email Reporting and Takedowns: NCSC & COLP receive reporting of suspicious emails from the public via SERS, which launched 21 Apr 2020. As of 31st March 2022, the number of reports received stand at more than 11,000,000 with the removal of more than 78,000 scams across 144,000 URLs. The public are sent large volumes of scam messages every day, many of which will be blocked by spam filters or otherwise ignored.

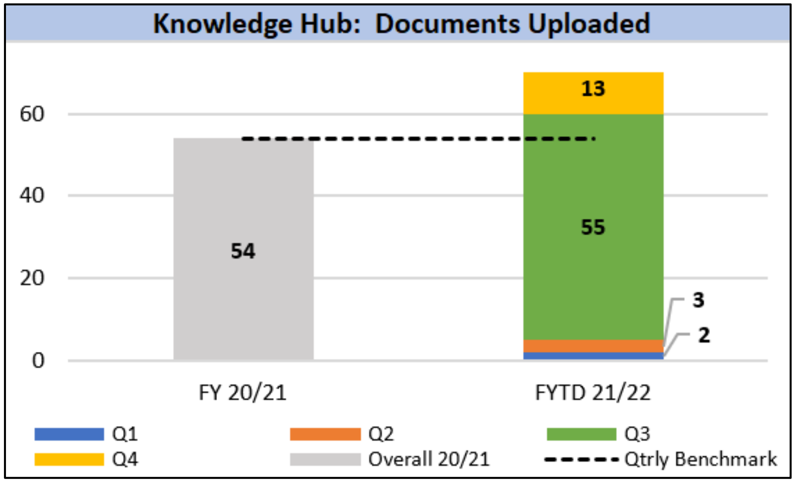
In Q4 there were more than 19,000 suspicious emails reported per day to NCSC and COLP, in addition to around 623 cyber-enabled crimes reported by victims to Action Fraud. From these suspicious emails, we identified nearly 340 new pieces of infrastructure (websites, servers, or emails) per day - i.e., about 1.8% of scam messages the public sent us contained unique knowledge of something malicious.

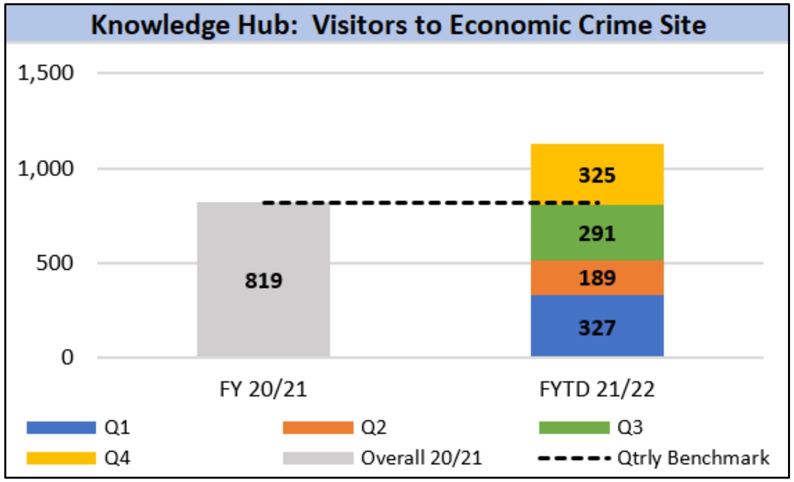
Outcome 5: *Policing has the capability and capacity to detect, disrupt and deter economic crime.*

NLF Role: City of London Police is a centre of expertise for fraud. It provides economic crime investigation training to policing, government and the private sector through its Economic Crime Academy. It is responsible for identifying, developing and disseminating good practice.

Success Measures:	
• Economic Crime Knowledge Hub engagement levels are increased	🟩


Knowledge Hub: New Members


Knowledge Hub: Documents Uploaded


Knowledge Hub: Visitors to Economic Crime Site

The Economic Crime Knowledge Hub membership has continued to rise steadily during Q4 2021/22. There have been 36 new members to the Economic Crime Knowledge Hub this quarter as the rate of new membership increased from Q3. The total membership fell following a purge of .pnn registered email addresses, but as below, the remaining members show high engagement levels with the site.

13 new documents were uploaded to the Knowledge Hub during the period, surpassing the total number of uploads from 20/21 by 35%. There were also 42 contributions to the site, including interactions on the forum and responses to polls, showing high levels of overall activity.

The number of visitors to the Hub has increased quarter on quarter since Q2, and the site welcomed 38% more visitors in 2021/22 than the previous year.

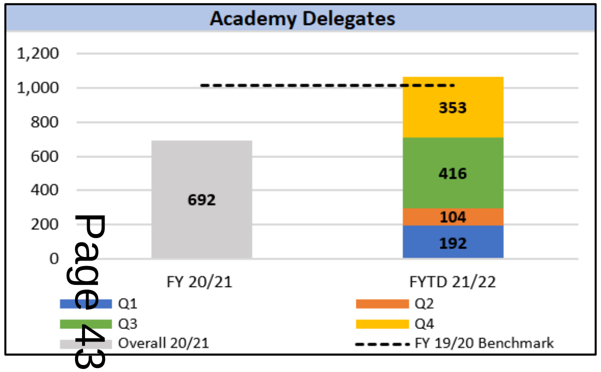
Outcome 5: *Policing has the capability and capacity to detect, disrupt and deter economic crime.*

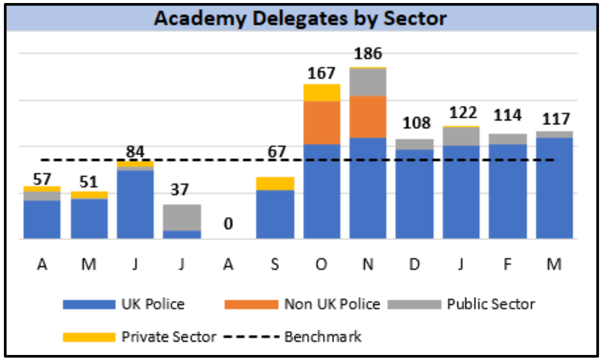
NLF Role: City of London Police is a centre of expertise for fraud. It provides economic crime investigation training to policing, government and the private sector through its Economic Crime Academy. It is responsible for identifying, developing and disseminating good practice.

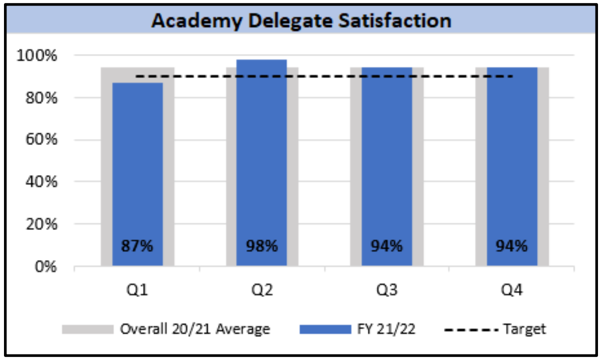
Success Measures:

- Delegate training numbers are sustained at 2019/20 levels* 🟩
- Delegate training has a 90% satisfaction rate. 🟩

*Stretch metric to increase these levels.







We have seen a sustained higher level of activity for the academy throughout Q4, taking the total number of delegates trained for the year above the 19/20 baseline and maintaining target levels of satisfaction. Across the period 32 courses were run and a total of 353 delegates attended from across UK policing and the public sector. We can see from the delegates by sector graph that after a slow start to the year delegate numbers have been above the benchmark level since October.

The ECA continues to adapt training to suit the needs of their customers, across the quarter a mix of face to face and online training has been delivered sometimes changing based on the request of the trainee organisation. Courses delivered included Bribery and Corruption, Money Laundering, Introduction to Economic Crime and Specialist Fraud Investigation (SFI).

March saw the ECA deliver its highest number of training days for the year across 11 courses. This included an SFI course in Manchester for delegates that are located outside of London. This course was very popular and as a result the academy have scheduled further SFI courses outside of London for the next financial year to meet the demand. A review of the course materials for the SFI course also began in March and good feedback , 96% satisfied, was received from an SFI course run online in February showing improvements over a previous online course which saw delegate satisfaction drop to 88%.

The ECA launched their Demystifying Cyber Enables Fraud course at the end of the year, and are looking to commission a Cyber Open Source Intelligence course as part of it's on-line offerings which will be offered to the NFIB.

This page is intentionally left blank

Committee(s): Economic & Cyber Crime Committee	**Dated:** 13/05/2022
Subject: Innovation & Growth – Update of Cyber & Economic Crime related activities	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1, 6, 7
Does this proposal require extra revenue and/or capital spending?	**No**
What is the source of Funding?	**NA**
Report of: Innovation & Growth	**For information**
Report author: Mary Kyle - Head of FPS Technology	

Summary

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

As the national lead force for fraud and cyber, the City of London Police (CoLP) plays a significant role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. This goes to the heart of the UK's competitiveness and so the work of IG and CoLP aligns.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime. It also highlights areas of cross-team working between IG and CoLP. Finally, the report puts forward a proposal for a new cyber project focused on supporting cyber security innovation to tackle emerging threats to business. This project will build on the recent work conducted by IG with Microsoft to support collaboration between FPS and cyber technology companies. Operating as a partnership between IG and CoLP, the project's main objective would be to strengthen the UK's cyber security credentials. This will be achieved by bringing innovative cyber security products to market and providing thought leadership on how to tackle emerging cyber threats to business.

Links to the Corporate Plan

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

Main Report

Innovation & Growth activity

<u>Digital Sandbox partnership with Microsoft</u>

2. In 2021 the City Corporation and Microsoft started exploring a joint challenge on the Digital Sandbox. We then co-hosted several workshops in late 2021 with financial services institutions. These were designed to identify a topic within the theme of cyber security where there was a joint interest across the financial services partners in developing technology solutions. A use case was agreed in February 2022 to focus on technology to support assessing, continuously monitoring and mitigating risks across the supply chain. Technology companies were invited to apply to participate in the Challenge. Five companies were selected – Risk Ledger, Orpheus Cyber, CyNation, arx Partners and Conatix.

3. Like the previous activities hosted on the Digital Sandbox platform, the primary aim of the Challenge was to foster collaboration between financial institutions and technology companies. In this case the collaboration was centred around addressing today's cyber security challenges and boosting the impact of measures to tackle cybercrime. By nurturing innovation in an increasingly important field, the Challenge sought to help UK business to lead from the front in adapting for the future. Specifically, the Challenge was designed to:
   (i) Cut across silos between traditional sectors and revitalise the ecosystem.
   (ii) Challenge organisations to work together on defining and solving a widespread problem statement; and
   (iii) Use the opportunities afforded by the Challenge, including the Digital Sandbox platform, to accelerate tech development so that it is market ready.

4. The Cyber Innovation Challenge operated on a closed basis with three financial services institutions engaging in weekly meetings with at least three of the five tech companies. These institutions included Nationwide and Hiscox. The weekly discussions formed a six-week sprint during which the participants had focused conversations to explore the solutions and how they could be developed to better meet the needs of the financial services sector. During this period the tech companies also had group collaboration sessions to provide them with further insights from across the cyber security eco-system. These included sessions with UK Finance, Osney Capital, London & Partners, Department for International Trade, Microsoft and City of London Police.

5. The Challenge culminated in a final presentation session bringing together all the participants. This provided the technology companies with a chance to present their solutions and explain how they had developed due to participating in the Challenge.

6. Initial feedback from the Challenge has been very positive. Successful outcomes include pilots that are now being conducted between some of the tech companies and the FS partners, improvements in the solutions that have been made because of the discussions that took place and ongoing exploration of possible partnerships between the tech companies themselves. All those involved in the Challenge who responded to the survey confirmed that they would recommend participating in the programme. All of those tech companies who completed the survey also confirmed that their involvement in the Challenge accelerated product development.

7. A public event to build out discussions around the use case and showcase the solutions that have come through the Challenge is being co-hosted by the City Corporation and Microsoft at Guildhall on 25 May. Officers in IG are in the process of preparing a full evaluation of the Challenge to review its success in meeting the

objectives set. This will also help inform any future iterations of this kind of Challenge.

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

8. We continue to use this report to review those activities which demonstrate the benefits of IG and CoLP collaboration. At the same time, IG is always alive to opportunities to promote the activity of CoLP and support their work as part of our wider stakeholder engagement.

<u>Collaboration</u>

9. Cyber Security Innovation Challenge – As referred to above, CoLP hosted a collaboration session for the tech companies involved in the Challenge. This provided the tech companies with an opportunity to better understand CoLP's role as national lead force for cyber. CoLP will also be represented on a panel as part of the 25 May event promoting the Challenge. As this event is aimed at a primarily business audience it will provide a good opportunity for CoLP to engage with the business community.

<u>Promotion of CoLP activity</u>

10. Officers in IG have been supporting CoLP ahead of a planned business breakfast briefing on 9 May. This has included reaching out to cyber and other business contacts to attend. The IG events team has also been supporting on logistics for the briefing.

Future Cyber Project

11. At the last Economic and Cyber Crime Committee meeting IG was asked to prepare a proposal for a future cyber project for consideration by this Committee. The aim of the project is to strengthen the UK's cyber security credentials by combining CoLP's strengths as national lead force for cyber with IG's FPS and innovation networks. Building on our work with Microsoft and the Cyber Innovation Challenge we are keen to explore a project that will support cyber security innovation to tackle emerging threats to business.

12. FPS remains one of the most targeted sectors for cyber attacks and these threats are constantly evolving. As the forms of attack become more innovative, there is an ever-increasing need for more innovative solutions aimed at the FPS market. There are many who are already working hard to develop products in this area. These range from across the FPS sector, BigTech and other fintech and cybertech specialists. However, there is significant scope to bring better products to the FPS market more quickly by supporting collaboration across these sectors.

13. Given CoLP and IG's aligned interests in supporting business we can see the benefits of partnering on delivery of a project in this area. Therefore, we propose to run an enhanced version of the Cyber Innovation Challenge to support collaboration and strengthen the pipeline of cyber security products aimed at FPS. The Challenge would consist of the following phases of activity:

    (a) **Initial partnership discussions** – the primary partnership driving forward the Challenge will be that between IG and CoLP. However, it would be worth exploring whether there are any other partners who either IG or CoLP would like to approach to bring in any broader expertise to the overall Challenge.

(b) **Objective setting** – IG, CoLP and any other partner will need to agree the objectives of the Challenge and how these will be assessed. From an IG perspective, key objectives will include accelerated product development, new partnerships and providing thought leadership on a topical issue. CoLP's objectives may be linked to increasing awareness of their role as national lead force and building out new business contacts, as well as providing thought leadership on key cyber security issues.

(c) **Challenge setting** – it is vital that the Challenge addresses an issue which resonates with businesses. Selecting a focus for the Challenge will start with discussions between CoLP and IG of those emerging cyber security threats to business that they are each aware of. CoLP and IG would then co-host several workshops bringing together those active across the cyber security space. This will include representatives from FPS, BigTech and cyber security companies, but also from Government, relevant trade associations and academia. At the end of the workshops the Challenge topic would be refined and finalised.

(d) **Challenge timetable development** – once the focus for the Challenge has been confirmed IG and CoLP will work together to build out a realistic timetable and programme of activity for the Challenge. Based on the feedback from the recent Cyber Innovation Challenge with Microsoft we would recommend running the Challenge over a 10-week period. The activity will consist of regular 1:1 sessions between tech and industry participants to work together on developing the solution. There will also be collaboration sessions led by key individuals and organisations active in the cyber security space to provide additional insight to those developing solutions. The Challenge will complete with a public showcase of the solutions that have been developed.

(e) **Industry participant confirmation** – to build out collaboration around the Challenge it is important to have a small number of very engaged industry participants. These partners will each be asked to sponsor at least two tech companies that are participating in the Challenge and work with them during regular 1:1 sessions to develop their solutions.

(f) **Technology participant applications** – we would suggest running a competitive process for bringing in tech participants to the Challenge. This would be open to any companies that are in the process of developing a solution that responds to the Challenge topic. Applications can be judged against several criteria including the solution's relevance to the use case, how innovative the approach is and the potential for the Challenge programme to support and accelerate development of the solution. This process would be run jointly by IG and CoLP, bringing in other third-party expertise to support where required.

(g) **Challenge finalisation and delivery** – once the industry and technology participants are confirmed then the Challenge programme can be finalised. CoLP and IG will take joint responsibility for delivering the programme. IG will be able to support based on experience running similar Challenges previously. CoLP's involvement will be key in terms of providing insight from their role as national lead force for cyber and exploring what data or other assets and information they may be able to share to support participants in the Challenge.

(h) **Challenge evaluation** – this will provide an opportunity to reflect on the Challenge and the extent to which it has met the objectives set at the outset.

14. There are differences between the recent Microsoft Challenge and the proposed Challenge. First, the partnership between IG and CoLP would be central to the Challenge, rather than CoLP playing a purely supportive role. Therefore, to take this proposition forward will require commitment from both parties to commit the necessary time resource to making it a success. Secondly, we would also look to have more input on this Challenge from other BigTechs and public sector interests from Government and regulators. Thirdly, the timeframe for development and delivery of the Challenge would be lengthened to allow more space for product development and data access to support this.

15. In terms of timeframe, if this proposal has the support of the Committee and CoLP then we could look to have initial discussions around partners and objective setting in June/July with a view to setting the Challenge, bringing in industry partners and running the tech application process in Q3/4 2022. The Challenge would then take place in Q1 2023.

Conclusion

16. IG is keen to explore ways to engage with CoLP. Collaborating on a significant project that aligns interests between the two teams will strengthen the working relationships already in place. It is also an excellent opportunity to pool our respective strengths and resources to support the UK's competitiveness at the forefront of cyber security.

Mary Kyle
Head of FPS Technology
Innovation & Growth
T: +44 (0)7834 808 240
E: mary.kyle@cityoflondon.gov.uk

This page is intentionally left blank

Agenda Item 13

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

Document is Restricted

This page is intentionally left blank

Agenda Item 14

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

Document is Restricted

This page is intentionally left blank

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

Agenda Item 15

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

Agenda Item 16

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

Document is Restricted

This page is intentionally left blank

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

Agenda Item 17

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Agenda Item 18

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

Agenda Item 19

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank