Public Document Pack

CITY OF LONDON

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

Date:	**MONDAY, 3 OCTOBER 2022**
Time:	**3.00 pm**
Venue:	**COMMITTEE ROOMS, 2ND FLOOR, WEST WING, GUILDHALL**

Members:
Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chair)
Alderman Professor Emma Edhem
Alderman Timothy Hailes
Dawn Wright
Deputy Graham Packham
James Tumbridge
Deputy Christopher Hayward
Deputy Graeme Doshi-Smith
Jason Groves
Alderman Bronek Masojada
Andrew Lentin (External Member)
Michael Landau (External Member)

Enquiries: **Richard Holt**
Richard.Holt@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/rjDDm43rb0M
A recording of the public meeting will be available via the above link following the end of the public meeting for up to one civic year. Please note: Online meeting recordings do not constitute the formal minutes of the meeting; minutes are written and are available on the City of London Corporation’s website. Recordings may be edited, at the discretion of the proper officer, to remove any inappropriate material.

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. **MINUTES**
To agree the draft public minutes and non-public summary of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May 2022.

For Decision
(Pages 5 - 10)

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

For Information
(Pages 11 - 12)

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

For Information
(Pages 13 - 18)

6. **NATIONAL LEAD FORCE PERFORMANCE REPORT Q1: APRIL – JUNE 2022**
Report of the Commissioner.

For Information
(Pages 19 - 36)

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

For Information
(Pages 37 - 44)

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

For Information
(Pages 45 - 48)

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

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

11. **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

12. **NON-PUBLIC MINUTES**

To agree the draft non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May 2022.

For Decision
(Pages 49 - 52)

13. **NON-PUBLIC OUTSTANDING REFERENCES**

Joint report of the Commissioner and Town Clerk.

For Information
(Pages 53 - 54)

14. **STRATEGIC COMMUNICATIONS & ENGAGEMENT: QUARTERLY UPDATE- ECONOMIC AND CYBER CRIME**

Joint report of the Commissioner and Town Clerk.

For Information
(Pages 55 - 60)

15. **NPCC CYBER CRIME PORTFOLIO- CYBER CRIME PLAN 2022-23**

Report of the Commissioner.

For Information
(Pages 61 - 68)

16. **NPCC CYBER CRIME PORTFOLIO- CRYPTOCURRENCIES AND VIRTUAL ASSETS**

Report of the Commissioner.

For Information
(Pages 69 - 74)

17. **NPCC CYBER CRIME PROGRAMME - BENEFITS EVALUATION 2021-22**
Report of the Commissioner.

For Information
(Pages 75 - 106)

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

For Information
(Pages 107 - 116)

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

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

Agenda Item 3

ECONOMIC AND CYBER CRIME COMMITTEE OF THE CITY OF LONDON POLICE AUTHORITY BOARD
Friday, 13 May 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 Friday, 13 May 2022 at 11.00 am

Present

Members:
Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chair)
Alderman Professor Emma Edhem
Dawn Wright
Michael Landau (External Member)
Deputy Graham Packham
James Tumbridge

Officers:

Pete O'Doherty	-	Assistant Commissioner
Nik Adams	-	Commander, City of London Police
Chris Bell	-	City of London Police
Emma Cunnington	-	City of London Police
Hayley Williams	-	City of London Police
Alix Newbold	-	Director, Police Authority
Oliver Bolton	-	Police Authority
Polly Dunn	-	Town Clerk's Department
Mary Kyle	-	Innovation and Growth

Observing:

Alderman Bronek Masojada	-	Member
Graeme Doshi Smith	-	Member
Jason Groves	-	Member
Sir Craig Mackey	-	External Member, City of London Police Authority Board

1. **APOLOGIES**
   Apologies were received from Deputy Chris Hayward and Alderman Tim Hailes. Andrew Lentin joined the meeting remotely.

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

3. **TERMS OF REFERENCE**

Members received the Committee's Terms of Reference as set by the City of London Police Authority Board at its meeting on 25 April 2022.

4. **MINUTES**

Michael Landau's name should be written in full on the attendance list.

RESOLVED, that subject to this correction, the public minutes and non-public summary of the meeting held on 14 February 2022, be approved as an accurate record.

5. **PUBLIC OUTSTANDING REFERENCES**

Members received a joint report of the Town Clerk and Commissioner.

The Commissioner noted that both items would be closed out soon.

RESOLVED, that the report be noted.

6. **NATIONAL LEAD FORCE UPDATE**

Members received a report of the Commissioner regarding the National Lead Force. An update was provided on the following matters:

- Procurement of the next generation Fraud and Cyber Crime Reporting and Analysis Service and the focus on Victim Care.
- Disruption of the sale of counterfeit goods and the challenges faced post-Brexit.
- COLP to report back on what further work could be done to intercept counterfeit goods in ports (e.g. working with Trading Standards) **(4/2022/P).**
- How the City of London Police planned to raise the profile of IP Crime, so that it might be taken more seriously.
- Threats to bypass Multi-Factor Authentication.
- Ongoing work on setting strategic objectives, with a view of fostering a more organised and co-ordinated response.

RESOLVED, that the update be noted.

7. **CYBER GRIFFIN UPDATE**

Members received a report of the Commissioner regarding Cyber Griffin.

It was clarified that the mission of Cyber Griffin was to engage with 100% of victims and that this work was undertaken by the wider team.

It was hoped that Cyber Griffin would be a product of the Cyber Resilience Centre Model, which will form one place for all services for large corporations and small SMEs.

Funding had been secured for this year but not beyond 2024 – it was suggested that Cyber Griffin may be self-funded in future.

A question was raised on whether there were any challenges with the Home Office, given that Policing is separate to Security. It was suggested that nationally, the direction of travel seemed to bring those two areas together.

RESOLVED, that the report be noted.

8. **Q4 NATIONAL LEAD FORCE PERFORMANCE UPDATE**

Members received a report of the Commissioner regarding the Q4 National Lead Force Performance.

The new Commander for Economic Crime, Nik Adams introduced himself and gave an overview of his previous experience in policing.

There was a discussion on the abandonment rate of calls and the need to improve the wait time of 12 minutes. This prolonged call-holding time was caused by low levels of contact centre staff. One reason cited for the lack of staff was the delay COLP is experiencing in the vetting process of new recruits. The City of London Police explained the need to prioritise the vetting process for data handlers to address this risk and added that this was being prioritised internally.

The Commissioner outlined the difficulties faced in domain blocking .com addresses compared to .co.uk. addresses. Processes were not as stringent although suppliers such as Go Daddy would take down sites if the evidence presented to them was compelling.

A Member sought a copy of the Police IP Crime report to the ICAN Board (**5/2022/P**).

A Member asked for an update on recruitment of Action Fraud Call Handlers outside of Committee, as the next ECCC is not until September. (**6/2022/P**)

RESOLVED, that the report be noted.

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

Members received a report of the Director of Innovation and Growth regarding an update on Cyber and Economic Crime related activities.

Members welcomed the development of a joint strategy with Innovation and Growth. They noted the convening power of the City of London Corporation and how this might help improve cyber consciousness.

Members invited COLP to consider what Members could do to assist in reaching businesses and suggested that links be made with relevant livery companies.

It was suggested that it would be useful for stakeholders to have one place to go to access all the relevant resources.

RESOLVED, that the report be noted.

10. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

11. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no other business.

12. **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.

13. **NON-PUBLIC MINUTES**
RESOLVED, that the non-public minutes of the meeting held on 14 February 2022.

14. **NON-PUBLIC OUTSTANDING REFERENCES**
Members received a joint report of the Town Clerk and Commissioner regarding the Board's Non-Public outstanding references.

15. **NATIONAL LEAD FORCE PLAN 2020-23- REFRESH**
Members received a report of the Commissioner regarding the National Lead Force Plan 2020-23 refresh.

16. **NPCC CYBER CRIME PORTFOLIO UPDATE**
Members received a report of the Commissioner regarding an update on the NPCC Cyber Crime Portfolio.

17. **STAKEHOLDER ENGAGEMENT PLAN- ECONOMIC AND CYBER CRIME**
Members received a report of the Commissioner regarding the Economic and Cyber Crime Stakeholder Engagement Plan.

18. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE - NEXT GENERATION AND CURRENT SERVICE UPDATE REPORT**
Members received a report of the Commissioner regarding the Fraud and Cyber Crime Reporting and Analysis Service, Next Generation and Current Service update report.

19. **NATIONAL POLICE CENTRE FOR ECONOMIC AND CYBER CRIME- VISION PAPER**
Members received a report of the Commissioner regarding the National Police Centre for Economic and Cyber Crime Vision.

20. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There were no questions.

21. **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 12.56 pm

Chair

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

This page is intentionally left blank

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/ Exec Dir for Innovation and Growth	It is requested that this OR be closed. I&G has explored this with the Lord Mayor's office, and at present there are no plans to host a Fin Tech event.
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.	Commissioner of Police	**Complete-** The Force's ABI funded Insurance Fraud Investigation Dept (IFED) has engaged with Cyber Griffin to explore opportunities and it has been raised at the General Insurance Fraud Committee (GIFC) by IFED in August 2022 which is supportive of using Cyber Griffin as a vehicle to progress this.
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 (Mary Kyle)	It is requested this OR be closed This comment was made by the previous Chair of P&R who has now moved on. Whilst I&G are in discussion with the Force regarding a new Cyber project as part of the Competitiveness agenda, there are no substantive proposals for a 'Centre for Cyber Excellence'. The advice from the NPCC Portfolio Lead was that the main focus should be on promoting the Cyber Resilience Centre for London. The Committee has been updated on the National Cyber Resilience Centre (NCRC) in previous updates.
4/2022/P	**13 May 2022** **Item 6**	COLP to report back on what further work could be done to intercept counterfeit	Commissioner of Police	**Complete**- The Police intellectual Property Crime Unit (PIPCU) is

Agenda Item 4

	National Lead Force Update	goods in ports (e.g. working with Trading Standards)		currently working with Border Force and the Intellectual Property Office (IPO) to conduct enforcement activity at the UK Borders. Additionally, PIPCU is also developing the intelligence picture to target the UK based transport activity that moves the counterfeit goods around the country.
5/2022/P	**13 May 2022** **Item 8** **Q4 National Lead Force Performance Update**	A Member sought a copy of the Police IP Crime report to the ICAN Board.	Commissioner of Police	**Complete-** There has been engagement with the Member - James Tumbridge. Meetings have been held and there is ongoing contact on this matter.
6/2022/P	**13 May 2022** **Item 8** **Q4 National Lead Force Performance Update**	A Member asked for an update on recruitment of Action Fraud Call Handlers outwith of Committee, as the next ECCC is not until September.	Commissioner of Police	**Complete-**An update on this was sent to the Clerk by Chris Bell on 21 June 2022 for circulation to Members of ECCC. It was noted at June PAB also that a regular update on this would be given under the Commissioner's update to each PAB until the position had improved.

Committee(s): Economic & Cyber Crime Committee	**Dated:** 3/10/2022
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: Damian Nussbaum, Executive Director Innovation and Growth	**For information**
Report author: Elly Savill, Policy and Technology Adviser	

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 NPCC lead for cyber, the City of London Police (CoLP) plays an important role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. The work of Innovation & Growth (IG) and CoLP therefore remains closely aligned.

The following report summarises the activity that has been taking place across IG in relation to cyber and economic crime, as well as cross-team working between IG and CoLP since the ECCC last convened in May 2022. The report includes a summary of the evaluation produced by CoLC and Microsoft regarding the Cyber Innovation Challenge. An update is provided on plans for a new cyber project focused on supporting cyber security innovation to tackle emerging threats to business. The project would be a partnership between CoLC and CoLP with a main objective being to strengthen the UK's cyber security credentials.

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/City of London Police cross-team working

2. We continue to use this report to review those activities which demonstrate the benefits of IG and CoLP collaboration. IG continues to look for ways to promote

the activity of CoLP and support their work as part of our wider stakeholder engagement.

Collaboration

3. The shift to hybrid working and lower levels of tourism have resulted in reduced footfall to the City. In response, CoLC launched Destination City, a new vision with the long term aim of rebuilding audiences, boosting the area's leisure offer and supporting the City visitor's economy. Destination City will be overseen by a newly appointed Destination Director, who will sit within IG. This will be a complex project, requiring ongoing dialogue and strategic collaboration with multiple levels of the CoLP. In the run up to Destination City's launch event, officers at the CoLP are already engaged at an operational level to ensure safety and security is at the heart of planning.

Promotion of CoLP activity

4. The Lord Mayor and Commander Nik Adams participated at the 39th International Symposium on Economic Crime, where they promoted the work of CoLC and CoLP in preventing both economic and cyber-crime through initiatives such as Operation Othello and Cyber Griffin.

5. As part of his trip to Australia, the Lord Mayor is planning to meet with Edward Kitt, FCDO lead at the Consulate on illicit finance. The Lord Mayor aims to use this opportunity to highlight the CoLP's role as the National Police Chiefs' Council Lead for Economic and Cyber Crime and their work at the forefront of efforts to combat money laundering, asset denial, and development of financial investigation capabilities. The trip was scheduled for September 2022 but following the passing of her Majesty the Queen, is in the process of being rescheduled.

Innovation & Growth activity

The Cyber Innovation Challenge

6. In March 2022 CoLC publicly announced the launch of the Cyber Innovation Challenge in partnership with Microsoft. The Challenge was a six-week sprint with financial services institutions and technology companies collaborating to develop solutions to assess and actively monitor the cyber security risks across the supply chain whilst also highlighting steps that can be taken to respond to any emerging threats. The Challenge was supported by sessions with UK Finance, Osney Capital, London & Partners, Department for International Trade, Microsoft and CoLP. The Challenge culminated in a final presentation allowing technology companies to present their solutions.

7. A public event to build out discussions around the use case and showcase the solutions that had come through the Challenge was co-hosted by CoLC and Microsoft at Guildhall on 25 May. Around fifty stakeholders and industry representatives were in attendance.

8. In the last update to the ECCC, IG reported that the team was in the process of undertaking a joint evaluation of the Challenge with Microsoft, to identify the success of the Challenge against a set of pre-agreed criteria. It also took into

account more general feedback and insight received from participants with a view to helping shape any future activities of this nature.

9. Initial feedback from the Challenge was very positive with successful outcomes including pilots being conducted between some of the tech companies and the FPS partners, an acknowledgement from tech company participants that the Challenge had accelerated product development and all respondents confirming that they would recommend participating in the programme. A more detailed summary of the evaluation's key findings can be found below.

Evaluation summary

10. The Evaluation aimed to shape any future activities of this nature by evaluating against a pre-agreed criteria consisting of the following themes: Thought Leadership, Financial Services Institutions (FSI) Involvement, Collaboration, Market Facing Impact, Outcome/Impact on Innovation. A summary of feedback for each of these criteria can be found below.

11. On thought leadership, CoLC and Microsoft evaluated this aim against whether the Challenge accomplished something that has not been done before and if the Challenge met a need that is currently not being resolved by the market. Feedback was positive, suggesting that while other programmes focused on supporting the development of cyber security solutions exist, they are not of the same nature and format of the Challenge. Additionally, there are no other programmes that focus specifically on this use case of developing tech solutions to help identify and mitigate cyber risks across the supply chain.

12. A key measure of the success of the Challenge was the engagement of the FSI sector which was largely successful. Moving forward, we believe there is scope to bring more organisations in to the workshop stage. Scheduling the Challenge and the specific times at which FSIs would be required to participate further in advance may also increase levels of involvement.

13. Fostering collaboration not just between the tech and FSI participants, but also with the broader industry partners was a key driver for Microsoft and CoLC launching the Challenge. Two of the three criteria set to evaluate the success of collaboration were achieved. These were goals relating to the total number of FSIs and technology companies involved in the Challenge as well as the level of engagement and collaboration. The third criteria regarded use of the Digital Sandbox. Feedback shows that whilst the Digital Sandbox platform was beneficial at the application and initial stages of the Challenge, it was not used to support collaboration between participants, with Teams and email acting as the preferred methods for collaboration and engagement.

14. Feedback regarding the criteria measuring market facing impact was mixed. Of the three tech companies which completed the exit interview, all confirmed that they had made or planned to make changes as a result of being involved in the Challenge and also stated that participation had accelerated product development. However, there was less consensus around the tech companies' ability to fulfil their testing plans with only two out of three confirming that their plan had been fully completed. Timeframe and a delay in hearing back from FSIs was blamed for this

issue. With this said, all tech companies that responded and the majority of FSIs and IGPs confirmed plans for continued engagement including demos.

15. Finally, measuring the outcome/impact on innovation was assed against whether the Challenge ended in steps that could be taken forward and if the Challenge provided further clarity on the issue in question. Feedback on both of these points was positive.

Future Cyber Project

16. The last report outlined proposals for a future cyber project for consideration by this Committee. This project would aim to build on the Cyber Innovation Challenge which sought to support cyber security innovation to tackle emerging threats to business. Championing this issue remains of the upmost importance as FPS continues to be one of the most targeted sectors for cyber-attacks, with bad actors constantly developing new methods for advancing cyber threats. The strategic outcomes of this new cyber project will be to:
    a. Accelerate development of innovative cyber-security solutions that meet FPS demand;
    b. Support cross-sector collaboration and information/data sharing on an emerging and/or key cyber-security challenge; and
    c. Provide thought leadership on catalysing cyber innovation in the UK.

17. CoLP have a unique insight into the cyber-security challenges that businesses face on a day-to-day basis as well as information on emerging cyber threats. It has therefore been recommended that this cyber project be a partnership between the CoLP and CoLC. This will be the key difference between the recent Microsoft and Challenge and this project.

18. CoLP will play an important role by providing cyber security expertise and identifying the use case. We believe that combining CoLP's strengths as national cyber lead with IG's FPS and innovation networks, can elevate this cyber project and help achieve the ambitions set out above, as well as meeting our shared interest of supporting businesses within the square mile.

19. Since the last update to the Committee, a detailed project plan has been drafted that sets out key aspects of the project such as the objectives, proposed roles, responsibilities, and scope of work. IG and CoLP are in the process of agreeing final details with regards to resources and timelines to ensure optimal utilisation and to maximise impact.

20. The project plan includes eleven different phases of work. While this is still yet to be agreed between IG and CoLP, it is expected that the core of the project will take place during 2023, with the possibility of phases 1-4 starting in Q4 2022.

21. The participation and expertise of CoLP will be key to the success of this project. Working in partnership, IG and CoLP are aiming to jointly present the final product for support at the next Committee meeting.

Conclusion

Collaborating on this new cyber project aligns interests between CoLP and CoLC, provides multiple moments in which to promote CoLP's work on cyber-crime and is an excellent opportunity to pool our respective strengths and resources to support the UK’s FPS to defend against emerging cyber threats. This will contribute to ensuring the UK remains the leading global financial centre.

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

This page is intentionally left blank

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Lead Force Performance Report

Q1: April – June 2022

Agenda Item 6

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

Performance Assessment

The dashboard provides an assessment of City of London Police (CoLP) performance against the National Lead Force (NLF) aims and objectives as set out in the National Lead Force Plan 2020-2023 (NLF Plan). The NLF Plan was approved by the City of London Police Authority in October 2020. The plan sets out how CoLP 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	**Supporting and safeguarding victims**	We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.	Overall - GOOD
Outcome 2	**Disrupt fraudsters**	We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.	Overall - ADEQUATE
Outcome 3	**Investigate and prosecute**	We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better outcomes for victims.	Overall - GOOD
Outcome 4	**Raise awareness and prevent crime**	We raise awareness of the threat and prevent fraud impacting people and businesses.	Overall - ADEQUATE
Outcome 5	**Building capabilities**	As National Lead Force we work creatively and with partners to improve capabilities to tackle fraud across policing and the wider system.	Overall - ADEQUATE

CITY OF LONDON POLICE

Performance Assessment

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 the 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 measure.

Table 1 – Success Measure Performance RAG assessment

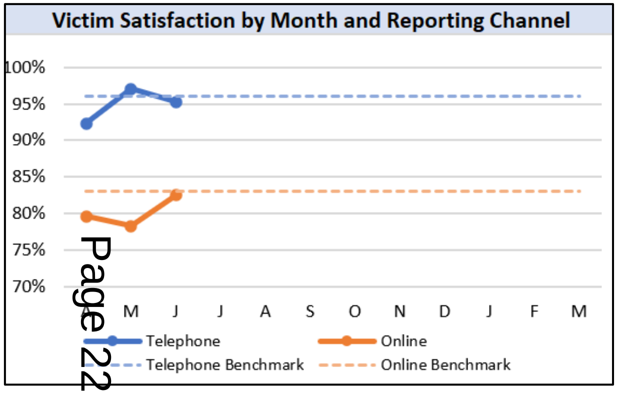
OUTSTANDING	Performance consistently exceeds expected success measures
GOOD	Performance consistently meets expected success measures
ADEQUATE	Success measures have not been consistently met but plans are in place to improve by the end of the period
REQUIRES IMPROVEMENT	Success measures have not been consistently met and there is insufficient evidence that performance will improve by the end of the period
INADEQUATE	It is unlikely the success measures will be met for the annual period based on the quarters to date
NO GRADING	Insufficient evidence means that no meaningful assessment is possible at this time

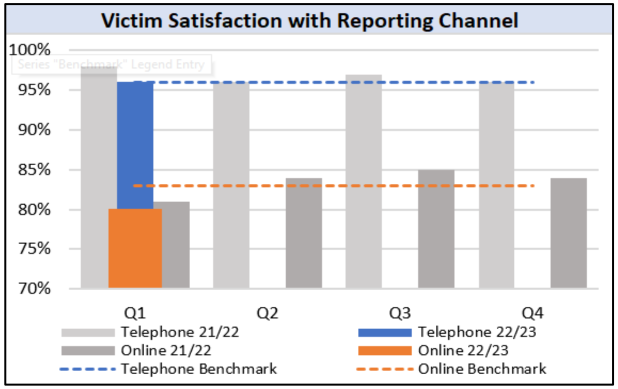
Outcome 1: *Supporting and Safeguarding Victims.*

NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

A.	To increase the percentage of survey respondents who are satisfied with the Action Fraud telephone reporting service.	GOOD
B.	To increase the percentage of survey respondents who are satisfied with the Action Fraud online reporting service.	ADEQUATE





Since the launch of the current victim satisfaction survey, Action Fraud advisors have provided a consistently good service. Overall, 0.8% of those reporting a crime in Q1 opted to provide satisfaction feedback to the confirmation fulfilment survey. Over 1.48M confirmation survey links have been delivered to date, with 16,606 respondents (1.1%) opting to provide satisfaction feedback, including free text responses which are used to continuously improve our service.

1.A. – The main Action Fraud survey indicates that satisfaction with telephone reporting service in Q1 remained within target at 96% despite a marginal quarter on quarter down trend of 17%, largely attributable to frustration regarding increased call wait times. However, this figure should be viewed with caution as April satisfaction metrics are unreliable and fell significantly due to technology issues associated with fulfilment amendment. During the period there was a slight improvement in both the average call handling time and the average speed of answer, and if these trends continue satisfaction would be expected to improve in Q2.

1.B. – Online satisfaction remained below target at 80% across the quarter with a June high of 82%. It should be noted that the technical issues affecting April/May fulfilment directly impacted the satisfaction responses provided. A workshop to review chatbot performance took place in June and any optimisation agreed will be put in place by the end of August.

CITY OF LONDON POLICE

Outcome 1: *Supporting and Safeguarding Victims.*

NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

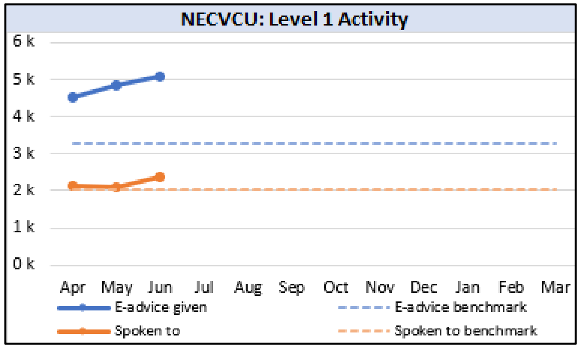
C.	To maintain the level of repeat victimisation after NECVCU contact to under 1%.	GOOD
D.	To increase the proportion of vulnerable victims receiving Level 2 support.	GOOD
E.	To increase the number of victims contacted by NECVCU.	GOOD

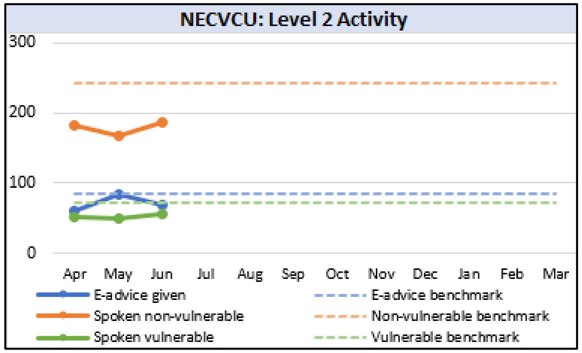
The National Economic Crime Victim Care Unit (NECVCU) supports forces at a local level, delivering care to victims of fraud and cyber-crime, allowing for a consistent and national standard of care and support. The **Level 1** service gives Protect/Prevent advice to non-vulnerable victims of fraud. The **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 a number of trials.

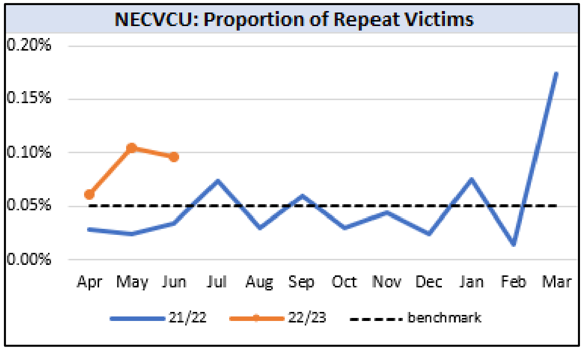
1.C. In Q1 there were 23 victims identified as repeat victims, up from the 2021/22 quarterly average of 9, but below the 1% target at 0.09% of victims engaged with during the period.

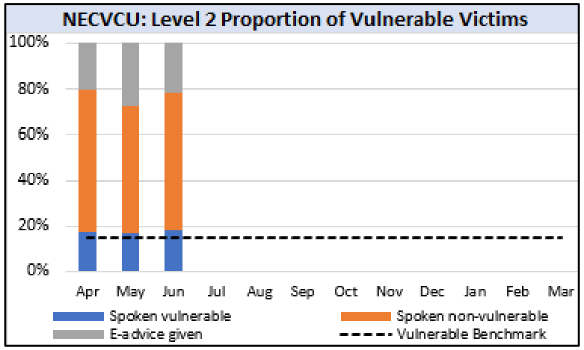
1.D. – The proportion of vulnerable victims spoken to by the Level 2 service was above the benchmark each month in Q1, with the quarterly total at 17% vulnerable victims, up from the 15% 21/22 average.

1.E. – When compared against the 2021/22 Q1 total (17,043) and the 21/22 quarterly average (19,931), victim engagement was up by 54% and 31% respectively, with 26,176 contacts across both levels.









Outcome 1: *Supporting and Safeguarding Victims.*

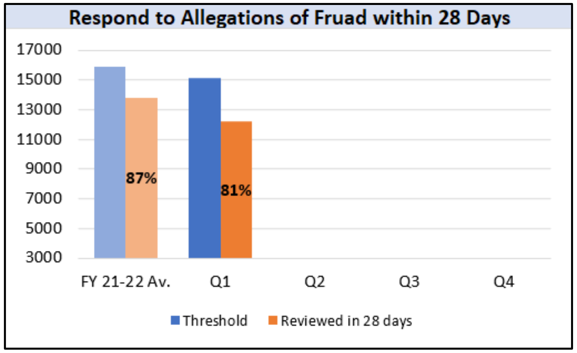
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

F.	To review and, where appropriate, disseminate for safeguarding or Protect activity, all victims that are identified as vulnerable, within 7 days.	GOOD
G.	To review and respond to all allegations of fraud that meet the threshold prioritisation criteria, within 28 days.	ADEQUATE
H.	To provide a fulfilment letter to all victims, within 28 days.	GOOD
I.	To send a bespoke Protect email to 95% of individual victims who provide an email address, within 7 days.	GOOD

1.F. – To identify potentially vulnerable victims, a search is run on all reports of fraud, looking at agreed 'risky words'.

In Q1, there were 3,128 reports identified as potentially vulnerable. 1005 of these were reviewed for vulnerability and 945 were sent to forces for Protect activity within 7 days of the report being downloaded to the system.


Respond to Allegations of Fruad within 28 Days

1.G. – The number of reports meeting the threshold for review dropped by 5% in Q1 from the 2021/22 average position. The proportion of these reports that were reviewed also dropped, from 87% in 21/22 to 81% in Q1. The main reason for the reduction in reviews is staffing reductions, including annual leave and high vacancies held in the team. There is an ongoing recruitment campaign and we expect this to even out over the rest of the year where leave periods are not so significant.

Trends with reporting are monitored. If a significant reduction in a particular crime type is noted, NFIB will look at options to encourage reporting to relevant sectors or individuals.

1.H. – 100% of fulfilment letters were dispatched to victims within 48 hours of the request being received.

1.I. – The NFIB have a number of advice letters, tailored to each fraud type, which are emailed to victims on a weekly basis. This service is known as 'Send in Blue'. In August 2021 this process was automated, and the success rate went from a low of 59% in June, to an average of 99.69% for the rest of 2021/22. In Q1 22/23, the success rate of Send in Blue was 99.88%.

Outcome 1: *Supporting and Safeguarding Victims.*

NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

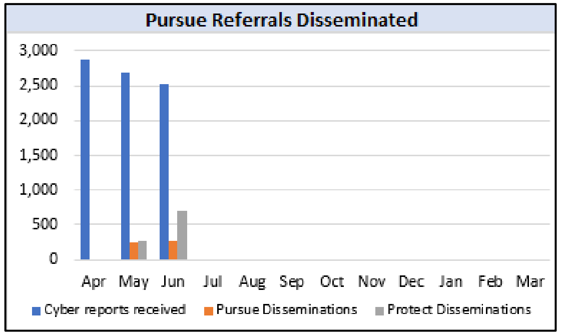
Success Measures:

J.	To review all unclassified cyber related Action Fraud reports to determine their viability for dissemination, within 7 days.	NO GRADING
K.	To review and disseminate all Action Fraud reports classified with an NFIB Cybercrime code, within 7 days.	INADEQUATE
L.	To respond to all live cybercrime reports, within 2 hours of reporting.	GOOD
M.	To determine and respond to all reports of cyber dependent crime identified as having a victims vulnerability factor, and disseminate for safeguarding activity, within 72 hours of reporting.	NO GRADING
N.	All businesses reporting cyber enabled crime to receive Protect advice within 72 hours of reporting.	GOOD

1.K. – In Q1, 8,072 reports were classified with a Cybercrime code. Of these, 19% were disseminated for Protect or Pursue. This measure is being reviewed and a process for reporting timeliness will be explored for Q2.

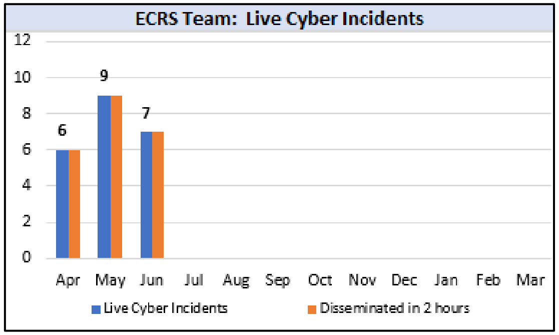
1.L. – 22 live cyber incidents were recorded in Q1, and each one was reviewed and a response sent within 2 hours.

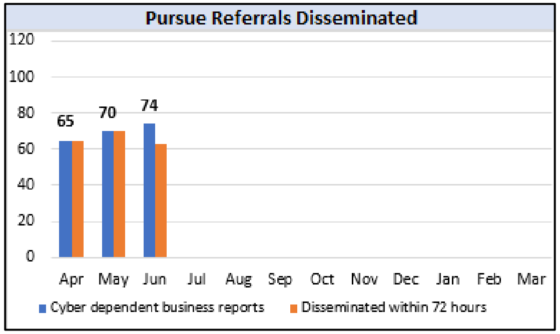
1.N. – 95% of businesses reporting cyber enabled crime were provided Protect advice within 72hrs. As the processes have become embedded this has improved to 100% consistently with bank holidays likely to be the only factor preventing this measure being met.



1.J. – NFIB Cyber are developing new management information processes to understand the demand and accurately report on the response.

1.M. – NFIB Cyber are currently reviewing the processes for identifying vulnerable victims which includes looking at the search terms used to identify those potential reports and retraining staff on Vulnerability, Domestic Abuse, Stalking, and Harassment. The new process for review and dissemination of reports by vulnerable victims is expected to be in place for reporting ahead of Q2.



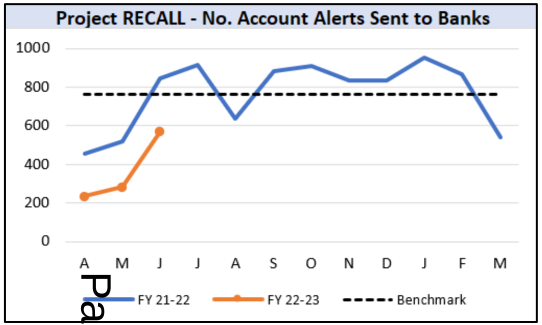


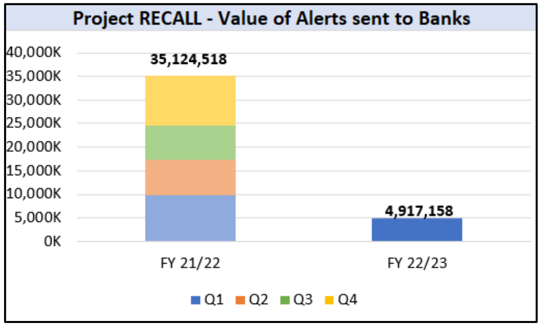
Outcome 1: *Supporting and Safeguarding Victims.*

NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

O.	To help victims of fraud to prevent or recover losses through information sharing with the banking sector and support from victim care.	ADEQUATE

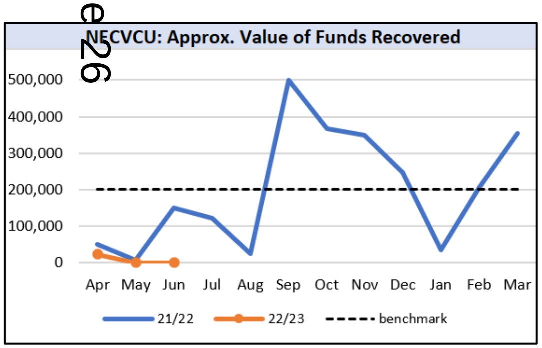

Project RECALL - No. Account Alerts Sent to Banks


Project RECALL - Value of Alerts sent to Banks

Project RECALL is a longstanding initiative to alert banks to accounts used in fraud. The number of disrupted bank accounts has been rising since the inception of the project, but a software licensing issue in April limited the number of alerts sent this quarter, despite steady recovery throughout May and June.

For the financial year to date CoLP have alerted banks of accounts used to receive the proceeds of fraud to the amount of £4,917,158. The system for banks to confirm the value of repatriated funds is not automated as yet, and in Q1 only £3 was confirmed to the NFIB.

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 2021.


NECVCU: Approx. Value of Funds Recovered

The number of **NECVCU** victims with confirmed recoveries, and the associated value of those recoveries is dependant on the victim informing the NECVCU. Since January 2021, 81 victims have reported approximately £2.5m refunds received.

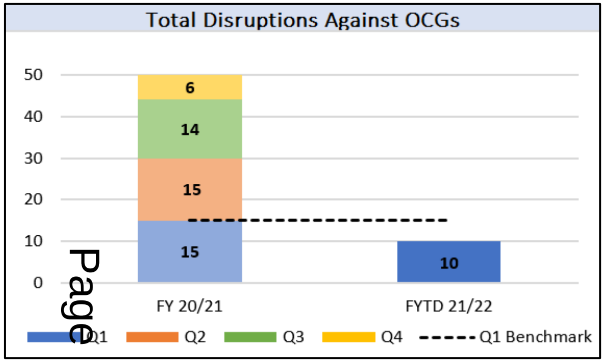
CITY OF LONDON POLICE

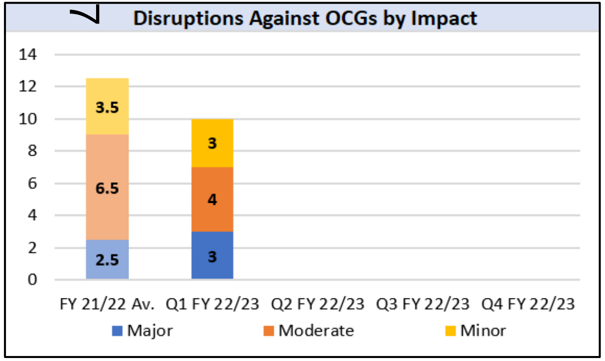
Outcome 2: *Disrupt Fraudsters.*

NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

Success Measures:

A.	To sustain the level of Economic Crime OCG disruptions.	ADEQUATE
B.	To increase the proportion of major and moderate disruptions against Economic Crime OCGs.	ADEQUATE





There are currently 63 mapped Organised Crime Groups (OCGs) under investigation by National Lead Force teams. Three new OCGs were mapped in the quarter, and five were closed.

There were 10 disruptions claimed against NLF OCGSs in Q1, which is less than the quarterly average of 12.5 from the previous year. Of these, 3 were classified as Major disruptions. There were also 4 Moderate and 3 Minor disruptions recorded.

There is currently only 1 Economic Crime OCG group that falls within the highest quartile of harm scoring OCGS and no disruptions were made against it in Q1.

It has been agreed that Met DCPCU Disruptions should be represented within these figures. These numbers are currently not included but are being retrieved, therefore the chart and figures are subject to future changes.

- A major disruption represents the OCG being fully dismantled or impacted at a key player level. Of the 3 Major disruptions claimed in Q1, 2 related to DCPCU OCGs, with the third mapped by PIPCU.
- 2 Moderate disruptions were claimed by DCPCU for large seizures, arrests, and intelligence development. PIPCU's Moderate disruption also included a warrant served, seizures and an arrest. The final Moderate disruption was claimed by IFED for 3 arrests, warrants and searches conducted, and seizures made.
- The Minor disruptions were claimed by PIPCU and the Fraud Teams for warrants, seizures and arrests made.

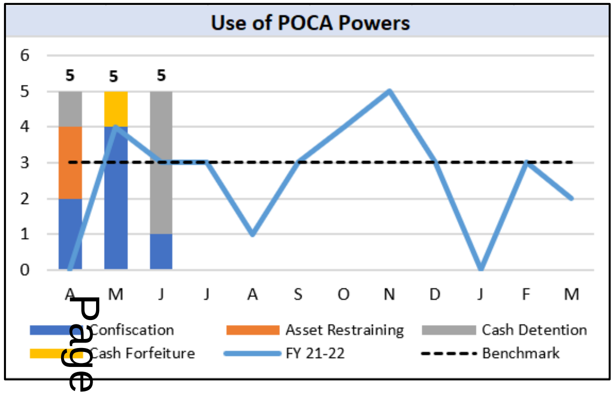
CITY OF LONDON POLICE

Outcome 2: *Disrupt Fraudsters.*

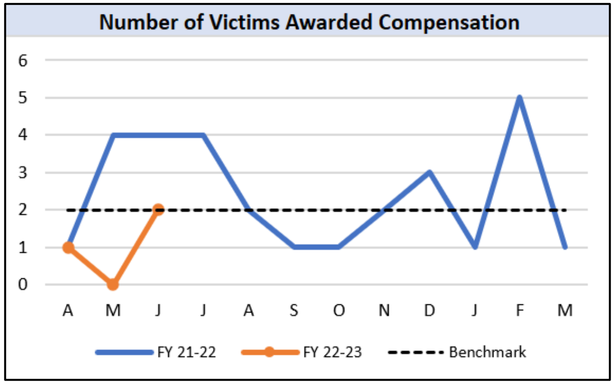
NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

Success Measures:

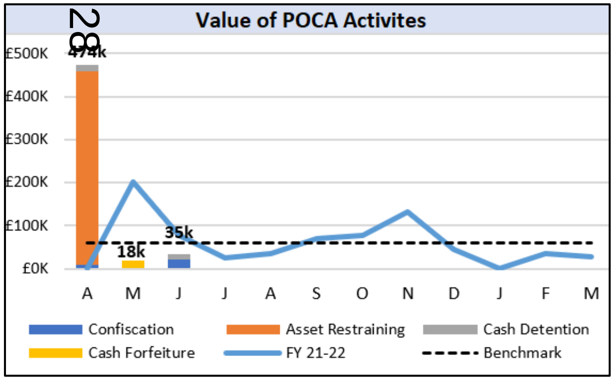
C.	To increase the use of POCA powers to freeze, restrain and protect proceeds of crime.	GOOD



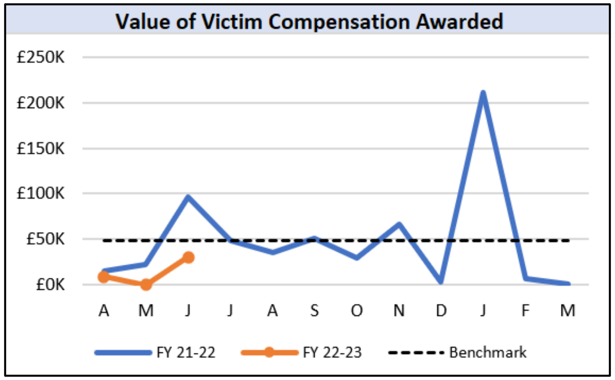
Use of POCA Powers



Number of Victims Awarded Compensation



Value of POCA Activites



Value of Victim Compensation Awarded

In Q1, Operational Fraud teams and Funded Units carried out a total of 15 POCA activities. This is above the 21/22 quarterly average of 8 and the 21/22 Q1 total of 7.

Most of the activity focused on confiscation orders (7) and cash detentions (5). However, the greatest value came from two asset restraining orders carried out in April. Following a DCPCU investigation into a criminal marketplace for software that gave fraudsters unauthorised access to compromised bank accounts, the suspect responsible was identified and arrested. As a result, police identified crypto assets valued at approximately £300,000 which have been seized and restrained. The Defendant pleaded guilty in June 2022 and confiscation proceedings are now ongoing.

Although below the 21/22 benchmark, teams worked to ensure that 3 victims were awarded a total of £39,598 compensation by the Courts.

CITY OF LONDON POLICE

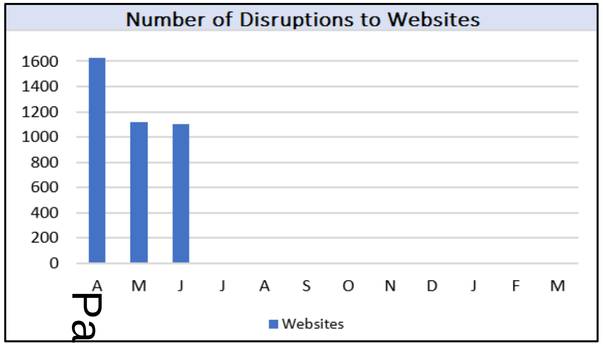
A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

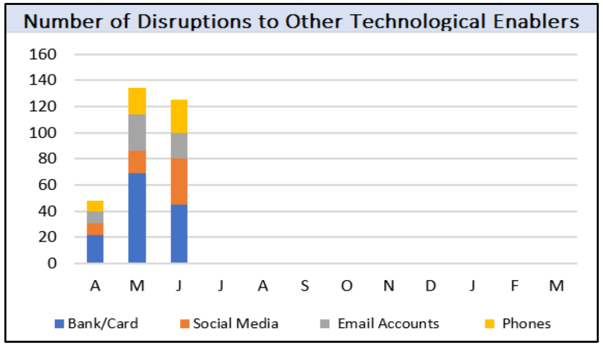
Outcome 2: *Disrupt Fraudsters.*

NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

Success Measures:

D.	To increase the identification and disruption of cyber enablers to curtail criminality and protect victims	REQUIRES IMPROVEMENT





During Q1, a total of 4,156 disruptions were recorded, a 39% drop from the 2021/22 Q4 total of 6,851. Disruption activity across departments focused on websites, both in the UK and overseas due to new partnership working from PIPCU. The NFIB Prevention and Disruption (P&D) team acts on referrals from Action Fraud, but the majority of its website disruptions are proactively sought.

Disruptions to other technological enablers rose throughout the quarter, reaching a peak in May. The P&D team is particularly aiming to increase disruptions to social media accounts used in fraud. They are working with the Home Office Economic Crime Directorates Homeland Security Group to build a direct relationship with Facebook, which will enhance the team's ability to make quick time disruption requests.

Calculating the value of 'actual loss' and 'potential loss saved' is complex and teams do not currently use the same methods. It is our aim to capture the impact of disruptions on victims and options are being explored to bring these in line.

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 30th June 2022, the number of reports received stand at more than 13,000,000 with the removal of more than 91,000 scams across 167,000 URLs. The public are sent large volumes of scam messages every day, many of which will be blocked by spam filters or otherwise ignored.

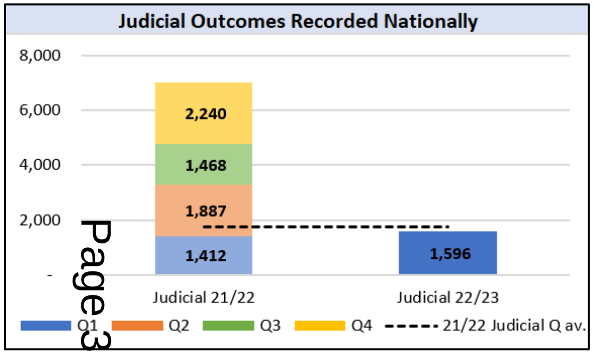
In Q1 there were more than 15,600 suspicious emails reported per day to NCSC and COLP, in addition to around 584 cyber-enabled crimes reported by victims to Action Fraud. From these suspicious emails, we identified over 330 new pieces of infrastructure (websites, servers, or emails) per day - i.e., about 2.1% of scam messages the public sent us contained unique knowledge of something malicious.

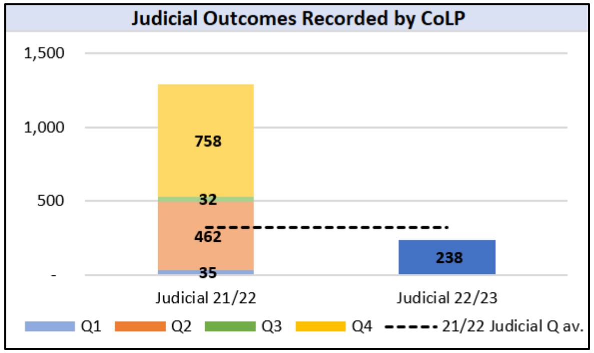
CITY OF LONDON POLICE

Outcome 3: *Investigate and Prosecute.*

NLF Role: We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better criminal justice outcomes for victims.

Success Measures:	
A. To maintain the level of Home Office forces in the compliant category for reporting at 100%.	GOOD
B. To increase the number of judicial outcomes recorded nationally by Policing.	GOOD
C. To increase the number of judicial outcomes recorded by City of London Police.	GOOD





At the end of Q1, the national judicial outcome rates are 7.6% for 2019/20, 5.0% for 2020/21 and 4.3% for 2021/22. There are still outstanding disseminations for each year either being investigated or awaiting closure - which means the outcome rate is likely to increase over time and these figures are subject to change.

The COLP judicial outcome rate is 22% for 2019/20, 9% for 2020/21 and 38% for 2021/22, far higher than the national averages. The COLP NFA rate is currently 5% for 2021/22, which is below the national average of 42%.

Although above Q1 21/22 levels, the number of judicial outcomes recorded locally and nationally falls below the quarterly average.

The total outcomes reported in the period can relate to disseminations from any time frame. The volume of outcomes is expected to fluctuate throughout the year as cases with varying numbers of crimes attached are seen in courts. For example, one investigation into a boiler room might have hundreds of outcomes attached to it and closing the case will give multiple outcomes and potentially bring closure to hundreds of victims.

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).

FY 22/23 FYTD	No. Forces
Compliant (2-3 Returns)	45
Partially Compliant (n/a)	0
Non Compliant (0-1 Returns)	0

Forces are required to provide outcome information to CoLP every month, matched against their NFIB disseminations. In Q1, all forces provide their return each month. The National Coordinators will continue to engage with forces to ensure this 100% compliance can be maintained throughout the year.

Outcome 3: *Investigate and Prosecute.*

NLF Role: We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better criminal justice outcomes for victims.

Success Measures:	
D. Through leadership of LFOR improve the coordination of Operational Activity across Policing to increase Pursue outcomes for victims.	ADEQUATE

Operation Henhouse was a National Intensification period that took place throughout May and early June. The Operation involved Forces and ROCUs targeting fraudsters by a period of enhanced PURSUE activity to increase arrests, voluntary interviews and disruptions linked to fraud, and the seizure and repatriation of the proceeds of crime back to victims. LFOR co-ordinated the National Policing response which resulted in an additional 186 arrests, 122 voluntary interviews, 353 cease and desist interventions and 131 seizures / Account Freezing Orders to the value of £33,088,81.

The development of the regional **Proactive Economic Crime Teams** continues to gather momentum with SW PECT coming on-line in Q1. The teams will focus on local, regional and national priorities, and make a significant difference in tackling fraud by adopting cases that may not reach investigative thresholds of other departments. LFOR oversee the Tasking and Co-ordination process for PECTs and will be introducing an APMIS based performance dashboard in the future.

LFOR assisted other Forces and Regions with **11 requests for assistance** during Q1 2022-23. The requests were for arrests, warrants to be executed, supporting premises searches, and the gathering of evidence. This is a key role of LFOR who will provide Operational and Investigative support to all UK Forces and Regions to progress cases with enquiries in London. A high number of OCG activity that impacts victims across the country have links to London, and by providing such support LFOR are supporting partners in expediting positive outcomes and disruption opportunities.

As the **National lead for Courier Fraud**, LFOR continue to support the Intelligence Development Team with analysis and dissemination of data to support PURSUE activity across the UK. The weekly bulletin, AMUR image circulation and National TEAMs call are examples of how NLF are co-ordinating the response to reducing Courier Fraud. These processes have enabled IDT to link offenders through the use of mobiles and MO which ultimately improve the opportunities for Forces to obtain a positive outcome by sharing key evidence and identifying new lines of enquiry.

LFOR received and developed 8 cases from UK Forces that were subject of **Case Acceptance Plans** for consideration by NLF Operations. This compares to 23 cases the previous quarter.

There have also been 49 **International requests for assistance** from Foreign Law Enforcement Agencies. These are managed within LFOR, and during this quarter the highest number of requests were from Germany. The overall number of International requests was 99 for Q4 2021-22.

Outcome 4: *Raise Awareness and Prevent Crime.*

NLF Role: We raise awareness of the threat and prevent fraud impacting people and businesses.

Success Measures:	
A. To Increase the number of Social Media posts.	ADEQUATE
B. To increase the reach of Social Media posts (impressions).	ADEQUATE

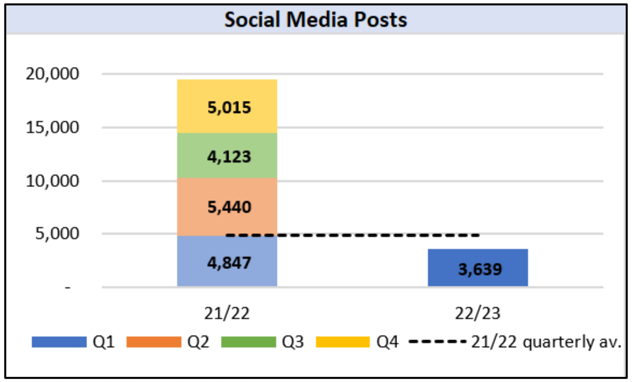
Across the various teams engaging on social media, the number of posts made were lower than the 21/22 Q1 and quarterly average. Engagement was also lower in terms of the number of impressions made, however activity did pick up towards the end of the quarter, driven in particular by the NFIB Cyber Protect team who saw 10,000,000 impressions in June alone.

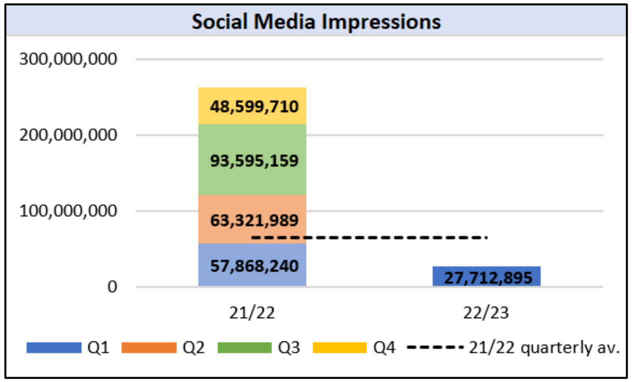
Notable campaigns included Cyber Protect's #remoteaccessscams, Action Fraud posted a number of alerts about the Ofgem phishing scam and launched campaigns on ticket fraud, holiday fraud and investment fraud. The Fraud and Funded units posted about their significant arrests and campaigns.

Across the quarter, the Media Team oversaw 16 press releases and 10 interviews, including newspaper and television interviews which resulted in positive news coverage. The NFIB also released 6 alerts through its digital community messaging platforms. These platforms reach approximately 350,000 users each time an alert is sent.

The Force continues to develop its understanding of engagement and reach for social media messaging. There are processes in place to collect data for the number of social media posts each quarter, and to record the numbers of impressions linked to these. Next steps will involve measuring the effectiveness of the content, analysing how to improve reach, and understanding whether behaviour will change as a result 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.





Outcome 4: *Raise Awareness and Prevent Crime.*

NLF Role: We raise awareness of the threat and prevent fraud impacting people and businesses.

Success Measures:		
C.	To deliver campaigns and participate in intensification periods to raise awareness and drive prevention activity.	GOOD

Lead Force Operations Room

LFOR co-ordinated the National Courier Fraud intensification period in April 2022. The majority of UK Forces and Regions participated in delivering PROTECT messaging to interested parties in order to reduce offending and highlight the impact on vulnerable victims. Courier Fraud is one of the identified priority offences due to the significant financial and emotional impact on the victims. The campaign received significant media attention and we continue to see a decline in reported offences of this crime type.

June 2022 saw the launch of the Crimestoppers and LFOR Courier Fraud awareness campaign. This is an initiative funded by the NECC that benefits from the established networks and Social Media platforms that Crimestoppers have previously developed. The campaign also provides an opportunity for the public to anonymously report any intelligence on those believed to be committing Courier Fraud. Raising awareness of Courier Fraud, identifying the signs and how to protect victims remains the key focus of the campaign.

LFOR continue to track emerging threats as identified in the NFIB threat assessment. COVID related fraud, travel insurance fraud, students engaged in money laundering (Mules) and fraud offences linked to charitable organisations exploiting the situation in Ukraine have all been identified. These will continue to be monitored and tackled via a series of PROTECT messaging via the RDO network and PURSUE activity tasked to the recently formed Proactive Economic Crime Teams.

Action Fraud

In the first half of 2022, Action Fraud has responded to emerging threats and trends by the regular dissemination of intelligence-led alerts via social media and the Action Fraud alerts service. In the first half of 2022, Action Fraud and Cyber Protect have delivered five national campaigns (Remote Access, Courier Fraud, Ticket Fraud, Holiday Fraud, Phishing) and collaborated on or helped to amplify national campaign activity from a host of partners, including the NECC, NCA, FCA and Gov.UK.

Alerts are informed and driven by the latest intelligence provided by NFIB. These can therefore be more "reactive" than the campaign activity which is planned in advance as part of an activity calendar. There will be occasions where the schedule is changed due to operational priorities, but it is mapped to coincide with seasonal demand or periods of operational intensification.

CITY OF LONDON POLICE

Outcome 5: *Building Capacity and Capability.*

NLF Role: As National Lead Force we work creatively and with partners to improve capacity and capability committed to fighting fraud, both across policing and the wider system.

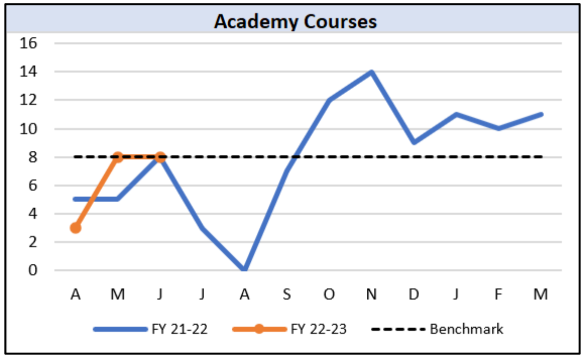
Success Measures:

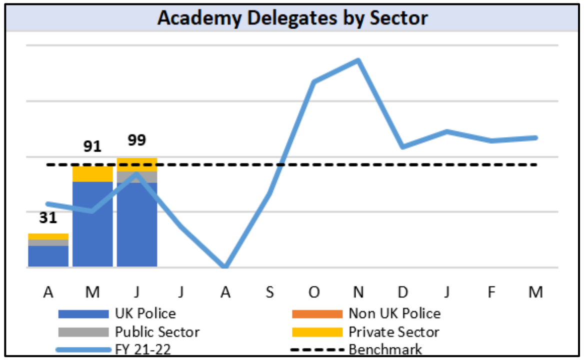
A.	To increase delegate training levels in the Economic and Cybercrime Academy.	ADEQUATE
B.	To maintain delegate satisfaction levels at 90% or above.	GOOD

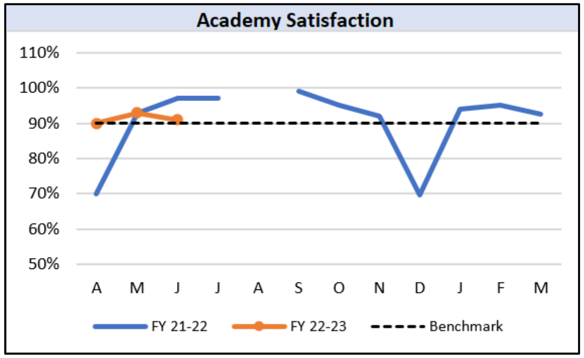
The ECCA delivered 19 training courses in Q1. As is often the case due to Easter and new budgets, April was relatively quiet, but the number of courses delivered in May and June was in line with the 2021/22 monthly average.

The number of delegates also increased throughout the quarter. 78% of delegates were from UK policing, with 14% from the private sector, and the remainder from the UK Treasury.

Satisfaction averaged at 91% for the quarter. Although mostly positive, feedback evaluation shows that delegates would prefer courses being delivered in the classroom rather than online.







In Q1, the Academy delivered a number of open courses, including Bribery and Money Laundering, Virtual Currency, Specialist Fraud Investigator (SFI), Fraud Investigators Foundation, and Internet Investigators Foundation Course. In addition, the first module of the Accredited Counter Fraud Specialist (ACFS) course was run, the first to be have given for nearly 3 years following Covid related delays.

Alongside these open courses Q1 also saw delivery of closed courses including Bribery to the NCA, Essentials of Fraud Investigations to NFIB staff, DCC to HM Treasury, and an online ML course to Thames Valley Police. June also saw the first investigative interview course of the year and the first Economic Crime Review course.

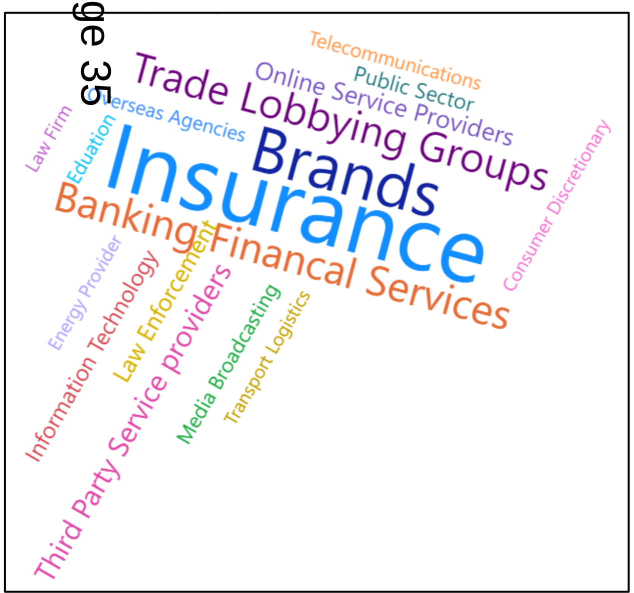
Outside the classroom, course development of the SFI course continues, along with development of a new online Cyber course that will be funded under Lloyds income.

Outcome 5: *Building Capacity and Capability.*

NLF Role: As National Lead Force we work creatively and with partners to improve capacity and capability committed to fighting fraud, both across policing and the wider system.

Success Measures:		
C.	To collaborate with industry and partners to develop innovative new ways to better protect victims and disrupt serious offending.	GOOD

There are two **COLP analysts embedded** in the NECC, and one in the NCA/NECC Multi Agency Fraud Targeting and Insight Centre (MAFTIC), targeting the highest harm fraud suspects in the UK and beyond. They have full access to AF/NFIB and policing data to target highest harm criminality, and a route into the 43 forces and ROCUs to expedite Pursue and Protect work. We also have embeds within our own teams from HMRC, Microsoft and shortly The Pensions Regulator to ensure that we are tackling fraud and cybercrime with a multiagency approach.



CoLP forms part of a multitude of **inter-agency groups** who tackle fraud and cybercrime in partnership. We work closely with a wide range of law enforcement and government agencies, banks, and industry partners, as shown in this diagram.

- The work of the **Intelligence Development Team** and their partners over the last three years has delivered huge success, especially with romance and courier fraud as part of the Project Otello campaigns. They continue to host national surgeries for law enforcement to share knowledge and issues, and to come together to tackle fraud.
- **Data innovations** in line with the National Policing Digital Strategy include our use of Project Droid to better handle big data. This has resulted in staff time savings, for example in the cyber mass disseminations process.
- Following evidence-based research, **financed by Lloyds Banking Group**, we licenced demographic segmentation data to better understand previous victims of fraud/cybercrime and thus identify chronic hotspots of victimisation. This means we can forecast potential victimisation by location, allowing forces the opportunity to conduct bespoke crime prevention outputs – an improvement to the one size fits all product previously completed. We now are working with 9 forces, delivering packages for Protect work in the hotspots we have identified, tailored to victims, with demographic data.
- The new **Enhanced Cyber Reporting Service** (ECRS) is providing a better service to business victims of cybercrime. The intel team are harnessing national Police Cyber Alarm data to understand the true threat to UK businesses from cyber attacks and attempts. The wider service will give a much more tailored and supportive approach to businesses which is then complimented by the wider cyber network, such as cyber resilience centres.

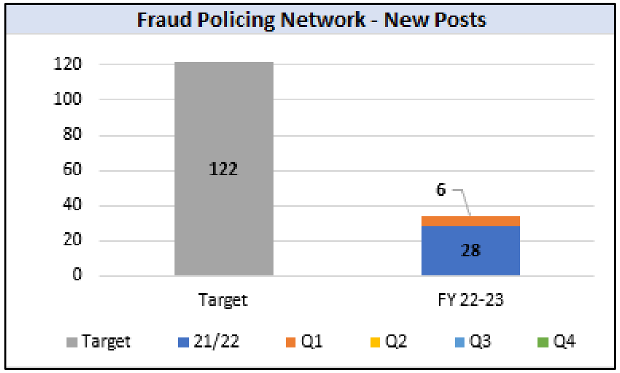
Outcome 5: *Building Capacity and Capability.*

NLF Role: As National Lead Force we work creatively and with partners to improve capacity and capability committed to fighting fraud, both across policing and the wider system.

Success Measures:		
D.	To improve the capacity to police fraud and cybercrime by implementing additional posts and improving attraction, recruitment and retention.	GOOD

Establishment of a new Fraud Policing Network (PURSUE) :

- Four proactive Economic Crime Teams (PECT) were established in four Regions during 2021-22 (Eastern, NW, West Mids, and Yorks & Humber). A total of 28 (Police Uplift Programme (PUP) funded) police officers are in post.
- A further six Regional PECTs are to be established in 2022-23 along with enlargement of the existing PECTs. By the end of 2022-23 the target is for the network to have 122 staff (through PUP and Spending Review Funding) across 10 Regions and CoLP NLF. At the end of Q1, 34 posts are in place (28%).
- The recruitment of five new posts into the NFIB Intelligence Development Team has been completed. These posts develop intelligence packages for the Regions and NLF, and support the tasking and coordination of cases across the Network.
- The Network performance framework in place, with ongoing refinement.



Additional recruitment and retention strategies currently being realised include:

- Having a clear development pathway for police staff working in fraud and cybercrime intelligence, from Researcher at grade C through to Director of Intelligence at grade G.
- Researchers and Analysts are all now booked on, or receiving, formalised research and analyst training. In addition there is regular Continuing Professional Development to maintain their skills and value to NLF/COLP.
- Regular opportunities arise for secondments and attachments with opportunities to grow knowledge and maintain the interest of police staff.
- Officers have been successfully supported through promotion processes over the last 24 months, feeling encouraged to achieve their goals and remain in the NLF as leaders.
- Quarterly Star Awards are presented as reward and recognition for NLF/NFIB staff and officers.

CITY OF LONDON POLICE

Committee: Economic and Cyber Crime Committee	**Dated:** 03 October 2022
Subject: National Lead Force Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1
Does this proposal require extra revenue and/or capital spending?	**N/A**
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 83-22	**For Information**
Report author: Peter O'Doherty Assistant Commissioner, 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

1. The National Lead Force Plan was approved by Police Authority Board in October 2020. Detail was given around new plans at the previous ECCC in September. The new performance measures are now in place and present on the accompanying performance report.

CURRENT POSITION

Outcome 1: Supporting and Safeguarding Victims.
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Next Generation service project update

The Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) programme is continuing to progress.
Remaining bidders are now forming their best and final offer bids for submission in early September. This is after an intensive period during June and July which seen all suppliers engaged in demonstrations and negotiations around their proposed solutions. The project remains on track to recommendation appointing preferred suppliers in November 2022.

Outcome 2: Disrupt Fraudsters.
NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

Cyber Prevention and Disruption Team

Disruption of a Sophisticated Recovery Room Fraud

Following a call to the force control room by a victim of fraud the Prevention & Disruption (P&D) team saw an opportunity to help disrupt a live fraud recovery room fraud. P&D officers contacted the victim and discovered that victims of an original land investment scheme fraud were being re-targeted by a sophisticated OCG purporting to be appointed by AF to support recovery of their funds. The suspects were cloning legitimate Solicitors firms and private asset recovery firms to encourage victims to part with further money for their services. The reporting victim was undergoing late stage cancer treatment and was highly vulnerable to such a sophisticated crime. Quick time action was taken to disrupt the suspects website, phone number and email address. An analyst was then tasked to research the Action Fraud System resulting in the identification of 29 AF reports and the opportunity to disrupt a further 10 phone numbers, 3 websites and 6 phone numbers used as vehicles for this crime. A further request was made to the complex crime team to review these AF reports for dissemination to force for investigation, with current losses report at over £600,000.

Disruption of Hacking For Mandate Fraud

P&D proactively identified the victim of a mandate fraud in which a legitimate Solicitors Firm was hacked and a number of their clients targeted with false invoices and payment requests resulting in losses exceeding £80,000 per victim. P&D noted a cloned website and email address created by the suspect to facilitate this and disrupted it, preventing further victims from being targeted. Officers then worked with the service provider to identify further websites and emails registered to clone other firms and removed these as well, preventing future harm. P&D are now working with the protect team to design alerts to businesses who may have been hacked for the purpose of mandate fraud and be unaware of the threat posed to their business and its customers. A further extension of this will be to explore the publication of protect alerts telling the public why a website has been taken down and encouraging the public to report if they have been a victim of crime.

Outcome 3: Investigate and Prosecute.
NLF Role: We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better criminal justice outcomes for victims.

PIPCU
Police Intellectual Property Crime Unit (PIPCU) and North West PIPCU led a week long intensification campaign to target the UK Counterfeit Hotspot in Cheetham Hill, Manchester under Operation Lucena. This was a multi-agency operation involving the IPO, GMP, Greater Manchester Council, and Immigration officer amongst others. The operation resulted in the arrest of 9 suspects, the seizure if over 28 tonnes of counterfeit goods with an estimated loss to industry of £20million. Over £18,000 cash was also seized. This resulted in extensive local media coverage and provided GMP with the opportunity to positively demonstrate the increased action that they will be taking in the area.

PIPCU
PIPCU executed a warrant at a warehouse thought to be selling counterfeit car parts. 1 arrest was made with 25 tonnes of goods seized and an estimated loss to industry of £1million. This resulted in the identification of an organised crime group that are also believed to be involved in other criminal activity, including money laundering.

National Lead Force
Op Rasalhague was an investigation into an investment fraud that was run by an Organised Crime Group targeting vulnerable people and repeat victims by using ‘sucker lists’. The victim was over 80, he lost £4m to fraudulent investments and the suspect tried to get another £67K from him, supposedly so the OCG could help him recover his money. The case was taken on by National Lead Force, City of London Police from other forces who were unable to provide a service to the victim. City officers visited the victim, prevented him from sending the further funds and provide crime prevention advice.

Intelligence development suggested the suspect was in Spain. The team worked with Spanish authorities to carry out overseas enquiries to locate and arrest him. An expert witness was engaged, he compared the recovered audio with calls recorded between the victim and suspect and with voice samples taken from the arrested person and confirmed them to be the same. This constituted part of the key evidence.

The suspect was remanded in custody and although he initially elected for trial, he later pleaded guilty to fraud. He was sentenced by HHJ Brown at Leicester Crown Court to two years immediate custody. The Judge praised the police investigation team, which comprised DC Howden and Police Staff Investigator Watkins and DS Meghji.

DCPCU - Cherokee

Background

A serial fraudster who impersonated genuine account holders (with counterfeit documents) was referred to the DCPCU to investigate.

Investigation

The investigation revealed that the fraudster was Mr Aadil LATIF. Between 29/01/2022 and 17/05/2022 Mr Latif had entered a number of Nationwide Branches in the North-West area of the UK and falsely purported to be customers and conducted withdrawals on the compromised accounts.

Mr Latif was arrested and charged for fraud.

On the 08th July 2022 at Liverpool Crown Court LATIF was sentenced to 14 months imprisonment.

DCPCU - Op Jade

Background

A corrupt staff member was identified as working with an OCG to unblock bank accounts that had security measures imposed on them by the bank. This is an MO the DCPCU are seeing more frequently where staff members are being corrupted to exploit accounts that are under the control of an OCG but have had blocks placed on them due to initial suspicious activity.

Investigation

The suspect was identified as Mohammed Iqbal who worked for the Palmers Green branch of Lloyds Bank.

Along with his co-conspirators Iqbal was responsible for a significant loss to the victims running into many hundreds of thousands of pounds.

Iqbal was seen in the branch with a number of co-conspirators and imposters who were variously posing as account holders or simply providing or exchanging information with Mr Iqbal to facilitate the frauds; changing account details and also authorising through, liaison with internal banking departments, fraudulent transfers that the bank had either blocked or highlighted as highly suspicious or potentially fraudulent.

Officers from the DCPCU arrested Iqbal and he was subsequently charged with fraud.

On Friday 22nd July 2022 at Snaresbrook Crown Court Iqbal was sentenced to 3 years and 6 months imprisonment.

IFED

R v **Rajesh Ghedia**

Rajesh Ghedia defrauded multiple insurance and pension companies out of over £1.3 million by feigning that he had stage 4 pancreatic cancer and less than a year to live. Ghedia also exploited his role at a well-known investment bank to convince friends, family and acquaintances to invest in financial products that did not exist. In reality, the victims had transferred nearly £625,000 directly into his personal account. Sentenced to a total of six years and nine months in prison and subject to confiscation proceedings.

Outcome 4: ***Raise Awareness and Prevent Crime.***
NLF Role: We raise awareness of the threat and prevent fraud impacting people and businesses.

City of London Police, as national lead force for fraud, launched a courier fraud campaign in May 2022 to raise awareness of the tactics used by callus fraudsters. A media pack including a press release, regional statistics and social media assets were sent out to forces to participate in the campaign.

Action Fraud launched a national awareness campaign on holiday fraud in May 2022 as new data showed reports had skyrocketed 120% between the 2020/21 and 2021/22 financial years.

Outcome 5: **Building Capacity and Capability.**
NLF Role: As National Lead Force we work creatively and with partners to improve capacity and capability committed to fighting fraud, both across policing and the wider system.

Economic and Cyber Crime Academy
New Webpage
The Academy Launched a new web page, complete with a new online booking system, that has incorporated the organisational step towards delivering 'Cyber Training' to UK law enforcement.

- Home | academy.cityoflondon.police.uk

The new web page reflects the change in organisational direction to include a wider Cyber Training portfolio and has been renamed to become the Economic and Cyber Crime Academy – *The ECCA'.*
The ambition is to be able to take on and lead the NPCC Cyber project training courses from October 2022.

To ensure we support Front Line Policing we have introduced several Continuous Professional Development (CPD) events. A 'bite size' 1 hour event where a current Threat, Harm or Risk is raised and discussed in partnerships with working regional partners, UK Finance, and the banking sector.
The first CPD was in relation to City of London Police and CPS agreed fraud best practice in the **Management and Risk Oversight Model for Serious and Complex Fraud.** The presentation reached 218 SIO delegates from across the UK to ensure that current best practise was circulated. It also supported HMICFRS Serious Organised Crime (SOC) inspection areas.

Internal training
Two free courses were provided to staff and police officers to improve the City of London Policing response to Cyber Crime and the open source intelligence available online.

- ECCA launches Open Source Intelligence course (sharepoint.com)
- Demystifying Cybercrime: Economic Crime Academy offer online course to all in force (sharepoint.com)

The Academy has introduced a training development programme for staff and officers to gain skills to deliver training commencing in September 2022

The Academy training team delivered the following courses to the following delegates in the first quarter supporting both National / Regional requirements and the PECT uplift of staff :-

Bribery and Corruption: 30
Accredited Counter Fraud Specialist Programme: 11
Virtual Currency Course: 53
Internet Investigations Foundation Course: 9
Demystifying Cybercrime: 12
Money Laundering: 53
Accredited Counter Fraud Manager: 13
Specialist Fraud Investigators Programme: 38
Fraud Foundation Investigation Course: 15
Investigative Interviewing: 7
Economic Crime Case Review: 15
Essentials of Fraud Investigation
A bespoke NFIB course : 9
Victim Care – 10

Funding

The Academy has secured funding to provide courses at 'zero cost' to support our National and Local policing colleagues over the next 2 years. It is hoped that this will enable staff/officers to be in the best position to tackle fraud and money laundering offences.

LFOR

LFOR led the National Courier Fraud campaign in May 2022

This generated considerable interest across the UK Forces and Regions. The campaign was heavily focussed on PROTECT messaging with the BBC, ITV, Radio 4 and a number of National and Local publications supporting the campaign in highlighting the issues to the public. As a direct result of the Safer Gem partnership in City of London, a 93yr old victim was prevented from losing £115,000 when he attended a jewellers who had been briefed on vulnerable victims and courier fraud as part of the campaign.

LFOR launched the Courier Fraud and Romance Fraud intensification period in partnership with CRIMESTOPPERS in June 2022.

This was an initiative funded by the NECC that utilised established networks such as Neighbourhood Watch and Social Media sites to support in LFOR in their role as National Lead for this offence. There has been a great deal of interest in the posts which has enabled LFOR to continue to reach out to all members of the Community in an attempt to reduce the offending and protect the vulnerable victims from being targeted. Latest NFIB figures show that Courier Fraud reporting is 61% lower than the average monthly figures for 2021-2022 and a 12% reduction from the previous month. The CRIMESTOPPERS campaign will shift focus to Romance Fraud in time for Christmas and Valentine's Day.

Proactive Economic Crime Teams

The number of Proactive Economic Crime Teams (PECT) that are operational continues to increase. Lead Force Operations Room (LFOR) has supported the recent development of South West ROCU, North West ROCU and TARIAN[1] PECTs and continue to manage the tasking and performance process on a National basis. We are in communications with East Midlands and the LFOR dedicated PECT officers working hard to identify and share best practice and any barriers that support the regions in their development of these pro-active teams. Eastern Region Special Operations Unit (ERSOU[2]) PECT recently obtained the first conviction for a male wanted initially for a breach of a Serious Crime Prevention Order but on further enquiries was committing other fraud related offences. He received a custodial sentence of 8yrs and 9 months.

Contact:

Kevin Ives

Detective Inspector

Staff Officer to AC O'Doherty

Kevin.ives@cityoflondon.police.uk

[1] Tarian ROCU – Regional Organised Crime Unit

[2] Home | ERSOU

This page is intentionally left blank

Committee: Economic and Cyber Crime Committee	**Dated:** 03 October 2022
Subject: Cyber Griffin Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1
Does this proposal require extra revenue and/or capital spending?	**N/A**
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 84-22	**For information**
Report author: Charlie Morrison, Detective Inspector, Head of Cyber Griffin	

Summary

Following a strong start to the year, Cyber Griffin is experiencing a temporary levelling-off of service delivery due to a challenging period for resourcing wider policing combined with meeting the changing demands from organisations in the Square Mile.

Positively, the programme is in the process of confirming stable funding from two sources (City of London Corporation Business Rate Premium and the National Police Chiefs Council (NPCC) Cyber Crime Programme). This funding will enable longer-term planning and the opportunity for Cyber Griffin to steadily increase the programme's impact on cyber insecurity.

The current unit remains two officers under-strength, though a recruitment process is engaged. One new officer is awaiting vetting clearance ahead of joining the unit. 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

Background

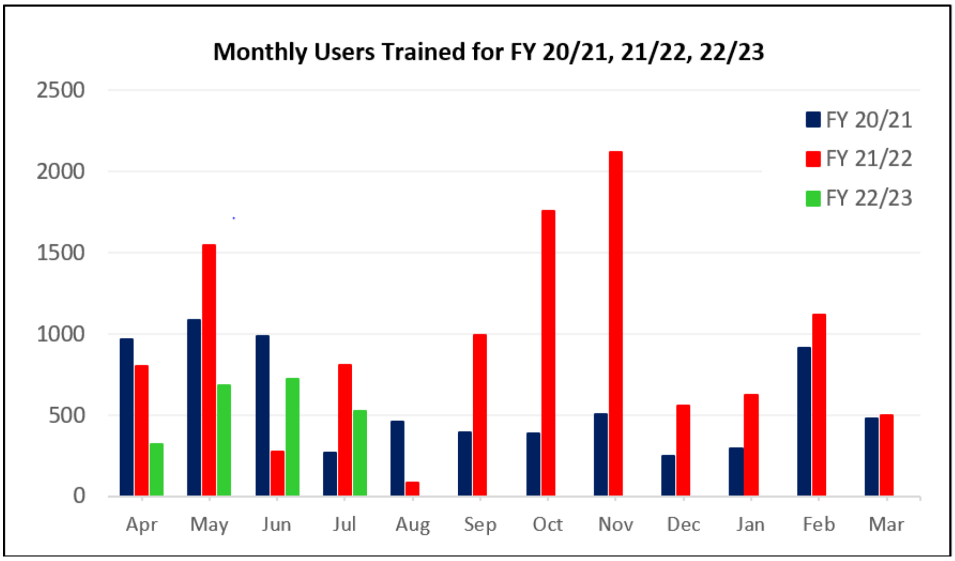
1. This Committee requested a regular quarterly report on Cyber Griffin activity. The report gives a brief update on the current position of the Cyber Griffin programme. For details of all Cyber Griffin services please visit: www.cybergriffin.police.uk

Current Position

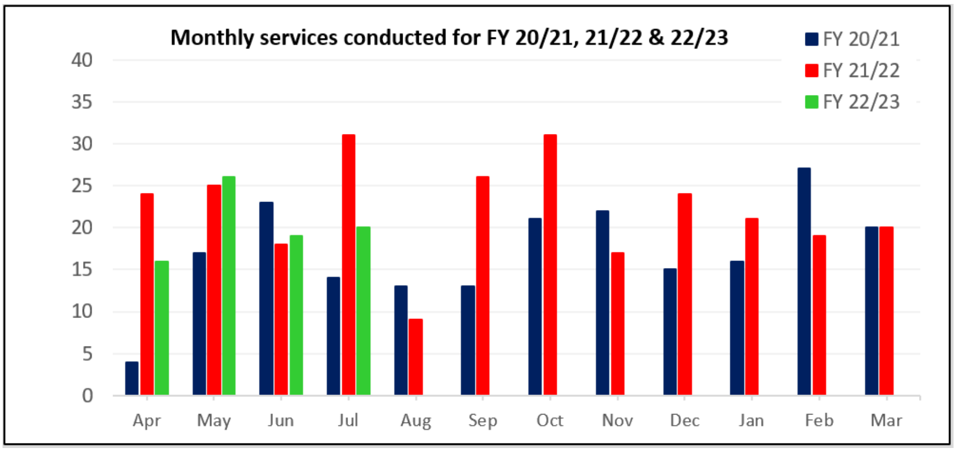
2. Whilst maintaining a good level of service over the last quarter +July, Cyber Griffin has not continued to exceed its performance compared with previous years. Abstractions to support cyber-dependant investigations and wider force deployments have been particularly high and consequently limited the team's opportunities to drive new engagements.

The programme has also experienced a significant change in demand over the last period. Organisations appear to have shifted their focus from staff awareness to incident response training and secure design. Subsequently, Cyber Griffin has delivered a far greater number of its services which deal with these security areas (namely: Incident Response Training and Cyber Capability Assessments). These more intensive services are delivered to smaller groups and aim to provide a longer lasting impact by encouraging the adoption of more secure policies, practices, and technologies organisation-wide. As demonstrated in graphs below this shift has led to a drop in the volume of people trained contrasted with a high number of services delivered.

Graph showing Cyber Griffin's monthly attendees compared with previous financial years



Graph showing the number of Cyber Griffin services delivered compared with previous financial years



3. Regarding locally set targets, the more ambitious annual targets set for Cyber Griffin remain achievable despite a challenging first quarter. The programme trained 2,316 people (quarter target – 2,500), conducted 86 services (quarterly target 67) and took on 46 new client organisations (quarterly target 36) in Q1. These figures have been adjusted to reflect the financial year as requested by the ECCC.

4. Regarding performance against national targets, Cyber Griffin continues to meet all nationally set key performance indicators (KPIs). Specifically, the programme has engaged with 100% of victims of cyber-dependent crime 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 considerably above 75%. Changes to national reporting have been announced and reviewed locally. It is believed that the extra anticipated demand is manageable with existing resources.

5. Looking ahead at performance, Cyber Griffin is forecast to go through an uncertain quarter. Wider policing demands are expected to continue having an impact on performance however, the coming months are also historically the busiest of the year owing to a greater interest in cyber security due to awareness campaigns such as cyber security month. It is not currently possible to say which of these two factors will have the greater influence on the quarter's performance.

6. Cyber Griffin's financial situation is extremely positive. The programme is in the process of confirming funding from both the City of London Corporation Business Rate Premium and the NPCC Cyber Crime Programme. Combined with the unit's current funding (due to end in April 2023), Cyber Griffin is likely to have stable long-term funding going forward. Meetings with senior officers are being arranged to discuss how the programme can use the advantage of stable funding to create long-term impacts on the digital security of the Square Mile. The outcomes of these meetings will feature in later reports.

7. Cyber Griffin continues to work with Bristol University in the development of a new Incident Response Exercise. The exercise algorithm is close to completion despite a series of setbacks relating to coding issues. 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 possibilities that the team have developed over the last three years. This marks a significant progression from traditional more linear 'paper-feed' exercising.

8. Finally, the protect advice landscape in London is due to change again as the London Cyber Resilience Centre (CRC) approaches its launch. This is a not-for-profit 'cyber protect' advice initiative supported by policing and the Home Office. Cyber Griffin remains in contact with CRC leads and will offer any support the initiative needs to establish itself in London's communities.

Conclusion

9. Cyber Griffin continues to offer a well-regarded and effective cyber security programme despite a challenging quarter and changes in the security interests of the Square Mile's community. As businesses continue to focus on incident response resilience and secure design, Cyber Griffin's focus will be to ensure these more intensive services meet the level of demand being placed on them. It is anticipated that the programme will be supported with stable long-term funding and consideration is being given as to how this positive development can be turned into developing a more impactive and effective Cyber Griffin offering. The next quarter is likely to see both a high demand for Cyber Griffin services and abstractions to wider policing demands. For these reasons it is difficult to estimate how the programme will perform against local targets. National key performance indicators (KPIs) will be maintained as a priority as these relate to victim response and care.

Contact:
Charlie Morrison
Detective Inspector
Head of Cyber Griffin
City of London Police

E: Charlie.morrison@cityoflondon.police.uk

Agenda Item 12

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 13

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 14

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 15

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 16

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 17

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.

Agenda Item 18

Document is Restricted

This page is intentionally left blank