



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

Date: FRIDAY, 8 SEPTEMBER 2023
Time: 11.00 am
Venue: COMMITTEE ROOM 1 - 2ND FLOOR WEST WING, GUILDHALL

Members: Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chairman)
Alderman Professor Emma Edhem
Dawn Wright
Deputy Graham Packham
James Tumbridge
Deputy Christopher Hayward
Sir Craig Mackey
Andrew Lentin
Nicholas Bensted-Smith
Michael Landau (External Member)
Jason Groves
Deputy Madush Gupta
Naresh Hari Sonpar
Michael Landau (External Member)

Enquiries: **Jayne Moore**
jayne.moore@cityoflondon.gov.uk

Accessing the virtual public meeting Members of the public can observe all virtual public meetings of the City of London Corporation by following the below link:

<https://www.youtube.com/@CityofLondonCorporation/streams>

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. Whilst we endeavour to livestream all of our public meetings, this is not always possible due to technical difficulties. In these instances, if possible, a recording will be uploaded following the end of the meeting.

Ian Thomas CBE
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 consider the public minutes and non-public summary of the Economic and Cyber Crime Committee held on the 11th of May 2023.

For Decision
(Pages 5 - 10)

4. **PUBLIC OUTSTANDING REFERENCES**

Joint report of the Commissioner and the 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 - 16)

6. **Q1 NATIONAL LEAD FORCE PERFORMANCE 2023-24**

Report of the Commissioner.

For Information
(Pages 17 - 36)

7. **NATIONAL LEAD FORCE AND CYBER UPDATE**

Report of the Commissioner.

For Information
(Pages 37 - 40)

8. **Q1CYBER GRIFFIN PERFORMANCE UPDATE 2023-24**

Report of the Commissioner.

For Information
(Pages 41 - 44)

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

10. **ANY OTHER BUSINESS THAT THE CHAIRMAN 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 consider the non-public minutes of the Economic and Cyber Crime Committee held on the 11th of May 2023.

For Decision
(Pages 45 - 48)

13. **STRATEGIC COMMUNICATIONS AND ENGAGEMENT PLAN FOR ECONOMIC AND CYBER CRIME**

Joint report of the Commissioner and Police Authority Director.

For Information
(Pages 49 - 74)

14. **ECONOMIC CRIME 5 YEAR STRATEGY AND POSITION AND ENGAGEMENT TO 2025 UPDATES**

The Commissioner to be heard.

For Information

15. **NATIONAL WORKFORCE/ PEOPLE STRATEGY UPDATE**

Report of the Commissioner.

For Information
(Pages 75 - 82)

16. **POLICE INTELLECTUAL PROPERTY CRIME UNIT (PIPCU) - UPDATE ON SCOPE OF ACTIVITY**

Report of the Commissioner.

For Information
(Pages 83 - 88)

17. **FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE -
PROGRAMME PROGRESS REPORT.**
Report of the Commissioner.

For Information
(Pages 89 - 94)

18. **TECH SECONDMENTS - OP ENLACE**
Report of the Commissioner.

For Information
(Pages 95 - 98)

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

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

**ECONOMIC AND CYBER CRIME COMMITTEE OF THE CITY OF LONDON
POLICE AUTHORITY BOARD
Thursday, 11 May 2023**

Minutes of the meeting of the Economic and Cyber Crime Committee of the City of London Police Authority Board held on Thursday, 11 May 2023 at 10.00am

Present

Members:

Deputy James Thomson (Chair)
Tijs Broeke (Deputy Chair)
James Tumbridge
Sir Craig Mackey
Andrew Lentin
Alderman Professor Emma Edhem

Officers:

Richard Holt	- Town Clerk's Department
Richard Riley	- Police Authority Director
Oliver Bolton	- Police Authority
Josef Shadwell	- Police Authority
Peter O'Doherty	- Assistant Commissioner, City of London Police
Nik Adams	- Commander, City of London Police
Michael Orchard	- City of London Police
Chris Bell	- City of London Police
Hayley Williams	- City of London Police
Lucy Cumming	- City of London Police
Elly Savill	- Department of Innovation and Growth

1. APOLOGIES

Apologies for absence were received from Deputy Christopher Hayward and Deputy Graham Packham.

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

There were no declarations of interest.

3. MINUTES

The Committee considered the draft public meeting and non-public summary of the previous meeting of the Economic and Cyber Crime Committee held on the 27th of January 2023.

RESOLVED- That the public minutes of the previous meeting held on 27th January 2023 be approved as an accurate record.

4. **OUTSTANDING REFERENCES**

The Committee received a joint report of the Commissioner and Town Clerk on the outstanding references from the previous meeting of the Committee.

RESOLVED- That the report be noted.

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

The Committee received a report from the Executive Director Innovation and Growth Department concerning activities that had been taking place across Innovation & Growth in relation to cyber and economic crime, as well as cross-team working between Innovation and Growth Department and the City of London Police since the Committee last met in January 2023.

Responding to a Member's question, Officers confirmed that the engagement between Innovation and Growth Department and City of London Police had been successful and that the teams had been successfully cooperating to ensure effective working and minimise efforts being duplicated.

The Chair commented on the value of working with strategic groups and asked Officers to propose strategies to the Committee at the following meeting so that they could make the most of their interactions with the Cyber Resilience Group, the City of London Corporation, and City of London Police.

RESOLVED- That the report be noted.

6. **NATIONAL LEAD FORCE Q4 PERFORMANCE REPORT**

The Committee received a report from the Commissioner concerning an assessment of City of London Police performance against the National Lead Force aims and objectives set out in the National Lead Force Plan 2020 - 2023.

Officers responded to Members query regarding engagement by confirming the details of the cross-sector communications and engagement strategy, spearheaded by the National Economic Crime Centre with support from the City of London Police, which would develop a national public campaign on fraud prevention messaging.

Replying to a Member's questions on performance measurement Officers explained that the Force would review grading assessments and performance reporting for the new financial year considering methodology to ensure assessments are fairly measured and to incorporate comments from the Committee. In addition, it was confirmed that measures were being taken to address the contact centre's shortage of staffing and consequent concerns with call answering and response timelines.

The Chair requested for a member briefing session (Deep Dive) on 'big issues' relating to Action Fraud and the implementation of the new Fraud and Cyber

Crime Reporting System. It was suggested this be held immediately before the September Police Authority Board.

RESOLVED- That the report be noted.

7. **NATIONAL LEAD FORCE AND CYBER UPDATE**

The Committee received a report of the Commissioner concerning information on key activities delivered as part of the National Lead Force Plan.

In response to a Member's enquiry regarding the scope and remit of the Police Intellectual Property Crime Unit, Officers confirmed that a short report on the activities of this Unit will be provided to the next Committee for information.

RESOLVED- That the report be noted.

8. **Q4 CYBER GRIFFIN PERFORMANCE**

The Committee received a report of the Commissioner concerning a record of the performance in Q4 compared to Q3 and the same period in the previous year.

RESOLVED- That the report be noted.

9. **COMMUNICATIONS & STRATEGIC ENGAGEMENT: QUARTERLY UPDATE**

The Committee received a joint report from the Commissioner and Town Clerk regarding key strategic meetings and events that have taken place between November 2022 and January 2023 which supported the Policing Plan's operational priority of protecting the UK from the threat of economic and cyber-crime.

The Committee discussed the need for proactive engagement with relevant stakeholders to improve and encourage visibility of the activities of the Economic and Cyber Crime Officers.

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 THE CHAIRMAN CONSIDERS URGENT**

Officers gave an update on the HMG Fraud Strategy detailing the three core aims of the Strategy, to ensure businesses, government and law enforcement gave consumers and people the tools needed to self-protect and to be aware of scams, requirement upon industries to early detect and disrupt enablers used to contact and defraud victims and legislation changes which would enable the implementation of the Fraud Strategy.

12. **EXCLUSION OF THE PUBLIC**

RESOLVED - That under Section 100(A) of the Local Government Act 1972, the public be excluded from the remainder of the meeting on the grounds that

the remaining items involve the likely disclosure of exempt information as defined in Part 1 of Schedule 12A of the Local Government Act 1972

13. NON-PUBLIC MINUTES

The Committee considered the draft non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 27th of January 2023.

RESLOVED - The non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 27th of January 2023 be agreed as an accurate record.

14. ECONOMIC AND CYBER POLICE HQ- PROGRESS UPDATE PAPER

The Committee received a report from the Commissioner concerning a progress update regarding the work to design a National Police Centre within the City of London Police for Fraud, Economic and Cyber Crime.

RESOLVED - That the report be noted.

15. FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE - PROGRAMME PROGRESS AND BUDGET SETTING REPORT

The Committee received a report from the Commissioner concerning the progress of the business case and programme of transformation of the Next Generation Service of the Fraud and Cyber Crime Reporting and Analysis service (FCCRAS).

RESOLVED- That the report be noted.

16. FRAUD AND CYBER CRIME REPORTING AND ANALYSIS SERVICE PROGRAMME - INFRASTRUCTURE AND PROJECTS AUTHORITY INDEPENDENT GATEWAY 3 OUTCOME REPORT

The Committee received a report from the Commissioner concerning Fraud and Cyber Crime Reporting and Analysis Service Programme – Infrastructure and Projects Authority Independent Gateway 3 Outcome Report

RESOLVED- That the report be noted.

17. NON-PUBLIC COMMUNICATIONS & STRATEGIC ENGAGEMENT: QUARTERLY UPDATE

The Committee received a joint report from the Commissioner and Town Clerk on the Communications & Strategic Engagement Quarterly Update

RESOLVED - That the report be noted.

18. QUESTIONS ON MATTERS RELATING TO THE WORK OF THE SUB COMMITTEE

There was no questions received in the non-public session.

19. ANY OTHER BUSINESS THAT THE CHAIR CONSIDERS URGENT AND WHICH THE SUB COMMITTEE AGREES SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED

There was one item of urgent business considered in the non-public session.

The meeting ended at 12:35pm

Chair

Contact Officer: Richard Holt
Richard.Holt@cityoflondon.gov.uk

This page is intentionally left blank

ECONOMIC AND CYBER CRIME COMMITTEE – PUBLIC REFERENCES

<p>2/2023/P</p>	<p>11 May 2023 Item 5- INNOVATION & GROWTH - UPDATE OF CYBER & ECONOMIC CRIME RELATED ACTIVITIES</p>	<p>The Chair asked Officers to propose strategies on how best to maximise the effectiveness of joint working with strategic partners (Such as Cyber Resilience Group and Corporation)</p>	<p>Exec Dir Innovation & Growth/Commissioner of Police/ Police Authority</p>	<p>Complete- CoLC and CoLP are continuing to identify and maximise opportunities for joint working. Examples are:</p> <ul style="list-style-type: none"> - Exploring economic crime roundtable with Anti-Fraud Champion and industry - CoLC raised awareness of work of Cyber Resilience Centres (CRCs) to stakeholders and I&G teams - Scoping projects on AI and economic crime with possible opportunity for partnership - Invited representatives from the CRCs to Cyber Innovation Challenge Showcase - CoLC invited representative from DCPCU to participate in panel at FCA/CoLC APP fraud event on 27th September - Joined up working across CoLC and with CoLP to draft lines on CoLC's position on economic crime
<p>3/2023/P</p>	<p>11 May 2023 Item 6- NATIONAL LEAD FORCE</p>	<p>The Chair requested for a member briefing session (Deep Dive) on 'big issues' relating to Action Fraud and the implementation of the new Fraud</p>	<p>Commissioner</p>	<p>This session as described will not go ahead for all Members. Instead, it has been agreed (at FCCRASP on 21st July) with Chairs</p>

ECONOMIC AND CYBER CRIME COMMITTEE – PUBLIC REFERENCES

	PERFORMANCE REPORT	and Cyber Crime Reporting System. It was suggested this be held immediately before the September Police Authority Board.		of FCCRASP and Chair of ECCC that the focus on these issues will remain with FCCRASP Committee and ECCC Members and detailed inputs will be given on agreed AF topics at the following FCCRASP meetings : 25 September 23 November 18 January To which ECCC Members will also be invited. An all Member Briefing can be offered nearer to 'go live'.
4/2023/P	11 May 2023 Item 7- National Lead Force and Cyber Update	In response to a Member's enquiry regarding the scope and remit of the Police Intellectual Property Crime Unit, Officers confirmed that a short report on the activities of this Unit will be provided to the next Committee for information.	Commissioner	Complete- there is a report on the agenda detailing this.

Committee(s): Economic & Cyber Crime Committee	Dated: 08/09/2023
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, Senior Policy and Innovation 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.

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 the City of London Police (CoLP) since the ECCC last convened in May 2023. The report includes examples of collaboration between CoLP and CoLC as well as updates on the Cyber Innovation Challenge.

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 to make the UK the safest place in the world to do business. 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. On 27th September, a representative from DCPCU will participate in a panel event at the CoLC and FCA event “Authorised Push Payment (APP) Synthetic Data Launch.” The panel discussion titled “A tour d’horizon of APP Fraud:

Enforcement and policing” will explore the evolving APP Fraud landscape with a focus on typologies, enforcement and policing and areas to improve collaboration.

Promotion of CoLP activity

4. In early September the Lord Mayor will speak at the annual Cambridge Economic Crime Symposium. Teams within CoLC have shared draft lines for the speech including the role of CoLP as the lead force for economic crime.

Innovation & Growth activity

Cyber Innovation Challenge 2.0

1. The Cyber Innovation Challenge provided a unique opportunity for financial services (FS) and tech companies with innovative tech solutions to collaborate over a six week sprint to develop technologies to address a security priority for the FS sector. As a reminder the Challenge use case explored by participants looked at the mechanism by which data is securely shared between the FS industry and law enforcement. More specifically:

How can technology capture live threat intelligence from financial services institutions and securely transfer this to law enforcement to improve oversight of threats facing industry? How can technology also provide a mechanism to share an anonymised update back to the wider FS sector to provide an enhanced insight into the threat level facing industry?

2. At the time of the last Committee meeting, the team were preparing to finalise 5-6 participating FS, open the application process for tech companies and finalise the Challenge timetable ready for the sprint to commence towards the end of June. An update on this is included below.
3. The team were pleased to welcome 5 FS to participate in the Challenge. They included Mastercard, Checkout.com, Clear.Bank and Legal and General. Representatives from 4 of the FS had been present during the industry roundtables held in February to identify the Challenge use case.
4. The application process for tech companies ran from 15th-31st May and was shared across CoLC and CoLP social media platforms as well as by Supporting Partners and industry bodies. Over 20 applications from UK and non UK tech companies were received – an increase on the first Challenge. On 5th June, representatives from CoLC and CoLP were joined by Supporting Partners Department for Business and Trade (DBT) and Microsoft to assess the applications and identify 5-6 successful applicants.

7 tech companies were chosen to participate in the Challenge. The tech solutions offered by these companies all approached the use case in slightly different ways. For example, some were better suited to the question of how data can be securely collected by FS and shared with law enforcement, some looked at data collection more generally and others could address the use case in full. However, it was agreed that all 7 tech companies offered innovative solutions. Once

companies had been notified of the outcome of their application and introductory session was held for successful techs to meet each other as well as the team from CoLP and CoLC.

5. The Challenge sprint commenced on 20th June with the opening presentations. Here the techs introduced their solutions to participating FS and Supporting Partners. Following the presentations the FS and techs were partnered up and went on to engage in weekly themed 1:1 discussions across weeks 2-5 of the sprint. The purpose of these 1:1s was for the techs to gain valuable feedback on the requirements of FS and for the FS to enhance the solutions to reflect their preferences and compatibility with their business. The weekly themes were assigned to help guide these discussions, they were: use case exploration and product limitations to overcome, data, product security and accessibility requirements.

In addition to the 1:1s, the techs benefitted from 6 collaboration sessions:

Collaboration session host	Theme
CoLP	Introduced the techs to the work and responsibility of CoLP as well as the system which would be replacing Action Fraud in Q1 2024.
Microsoft	Former RickIQ employee described experiences of acquisition by Microsoft and how they scaled. Microsoft also introduced a range of support offered to tech sector.
DBT	Introduced the support DBT offers the tech sector to export around the world.
Microsoft	Looked at the importance of ensuring products are accessible to the needs of different users.
London and Partners	Explored the support “Grow London” can offer SMEs to scale.
ICO	Introduction to the ICO Innovation Hub and discussion on UK data regulation.

Although not a Supporting Partner, the team felt that the significance of data in this year’s use case warranted engagement with the ICO as this would allow the techs to discuss data sharing and handling requirements directly with the regulator.

6. On 2nd August, the sprint concluded with the closing presentations. These highlighted a variety of the tech’s learnings including better understanding of the technical preferences of FS, improved understanding of FS governance and compatibility requirements, an improved understanding of the data CoLP would find most beneficial from businesses and the support on offer for the tech sector to scale and export.
7. Although the sprint has ended there are two final steps to complete before we conclude this project. The first is the showcase event taking place on Tuesday

19th September, Guildhall. The agenda and speakers have been finalised and include a selection of handpicked techs and FS. While the event will be held under Chatham House rules, the team are working on some possible comms to be shared on the day and following the event. The second is the Challenge evaluation which will capture feedback from participants and Supporting Partners collected throughout the Challenge. This is an important tool in identifying the accomplishments and areas of improvement for future iterations. We aim to have the evaluation drafted in early Q4 meaning an update will be available for the next Committee.

Conclusion

The Cyber Innovation Challenge has been a collaborative effort between CoLP and CoLC and has showcased our shared objective to support industry and ensure London and the UK is a safe and secure place to do business. The project created a unique platform for collaboration to explore an ambitious use case and the team now looks forward to welcoming Members to the showcase and sharing findings from the Challenge evaluation.

Elly Savill

Senior Policy and Innovation Adviser

Innovation & Growth

T: +44 (0) 7500 785073

E: eleanor.savill@cityoflondon.gov.uk

National Lead Force Performance Report

Q1: April – June 2023
Page 17



Agenda Item 6

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' effort to drive down 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: -






			Data Trends
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.	➔
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.	⬆
Outcome 3	Investigate and prosecute	We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better outcomes for victims.	➔
Outcome 4	Raise awareness and prevent crime	We raise awareness of the threat and prevent fraud impacting people and businesses.	⬆
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.	➔



The grading criteria can be found in Appendix A – Performance Assessment Criteria



Executive Summary

Outcome 1 	Outcome 2 	Outcome 3 	Outcome 4 	Outcome 5 
Supporting and safeguarding victims	Disrupt fraudsters	Investigate and prosecute	Raise awareness and prevent crime	Building capabilities
<ul style="list-style-type: none"> A. Action Fraud phone satisfaction improved due to faster speed of answer and lower call waiting. B. Online satisfaction consistent. C. Lower levels of NECVCU repeat victims in Q1. E. Increase in no. forces supported by NECVCU and consistent escalations. F. 90% Vulnerable Person Alerts sent in 7 days. G. 31% highly likely reports reviewed in 28 days, with disseminations increasing. H. 100% victim updates sent. I. 96% cyber reports disseminated by the target 7 days. J. 80% of live cyber incidents responded to in 2 hours due to 1 exception. K. 95% Protect advice sent in 72 hrs L. Number of Recall alerts sent above 22/23 average. 	<ul style="list-style-type: none"> A. The number of disruptions against OCGs were in line with the 22/23 average. B. Total disruptions against OCGs and SOC strategic vulnerabilities surpassed both Q1 22/23 and the quarterly average. B. Proportionally, Q1 saw an equal number of Major disruptions to OCGs from the 22/23 average, and an increase in Moderates. C. The number and particularly value of POCA activities increased from 22/23 and included cryptocurrency. D. Disruptions against cyber enablers fell overall from Q4 22/23, however, volumes do fluctuate and are expected to rise. 	<ul style="list-style-type: none"> A. The number of judicial outcomes that were recorded nationally was in line with Q1 22/23 and the 2/23 average. B. Following a high volume of CoLP outcomes in Q1 22/23 outcomes in Q1 23/24 were low. However due to fluctuations in reporting throughout the year, it is expected that this will improve over the next few quarters. C. All 45 forces remained compliant in reporting their outcomes. D. LFOR reported good performance consistently across the range of their activities, this includes coordinating national campaigns. 	<ul style="list-style-type: none"> A. The number of social media posts was higher than any quarter in 22/23 showing a broad range of messaging across all teams. B. The related impressions are equal to the 22/23 quarterly average. B. In addition, 17 press releases were issued. C. Two very successful campaigns were run, targeting both romance fraud and courier fraud, working with partners to drive prevention activity. C. Additional two Protect campaigns focused on holiday fraud and phishing, raising the public's awareness. 	<ul style="list-style-type: none"> A. ECCA provided more courses to an increased number of delegates compared to Q1 2022/23. B. ECCA satisfaction was slightly below target but expected to improve. C. NLF demonstrated a wide range of collaborations in Q1. D. PECT teams staffing moved closer to the end of year target, and teams demonstrated positive results in the period.



The grading criteria can be found in Appendix A – Performance Assessment Criteria



Outcome 1: Supporting and Safeguarding Victims.

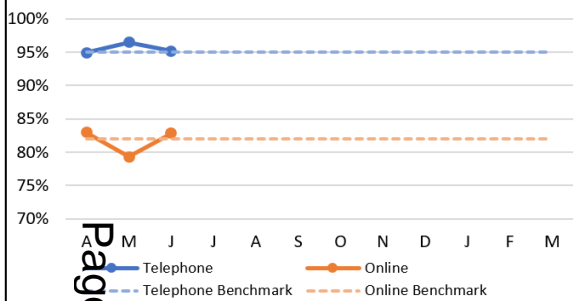
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

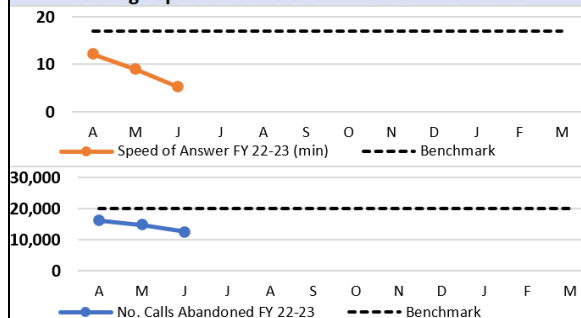
- A. To provide a consistent level of satisfaction with the Action Fraud telephone reporting service.
- B. To provide a consistent level of satisfaction with the Action Fraud online reporting service.



Victim Satisfaction by Month and Reporting Channel



Average Speed of Answer and Call Abandonment



Since the launch of the current victim satisfaction survey, Action Fraud advisors have provided a consistently good service. Overall, 1% of those reporting a crime in Q1 opted to provide satisfaction feedback to the confirmation fulfilment survey. Over 1.82M confirmation survey links have been delivered to date with over 20k respondents (1%) opting to provide satisfaction feedback including free text responses, which are used to continuously improve our service.

Telephone Reporting Service - In order to provide a consistent level of satisfaction with the telephone reporting service, Action Fraud have implemented several improvements to enhance the user journey and accessibility into the service, such as Language Line and the Sign Video reporting option for Deaf users. The Advisor XP Contact Centre tool was also launched in Q1, a chat bot style tool offering advisers real time support, to ensure that victims are provided with correct advice and referrals. These are expected to improve the quality of calls and reduce call waiting and handling times, which should in turn increase victim satisfaction.

Q1 saw a significant uplift in contact centre staff numbers which resulted in an upward turn in performance and a reduction in call abandonment to 33% from 49% the previous quarter. The additional staff have answered just under 20k additional calls compared to Q4 22/23. Call handling times have reduced by 8% from Q4 to an average of 21.74 minutes, and the average speed of answer has reduced by 50% to 8.83 minutes. The average speed to abandonment in Q1 was 5.94 compared to the previous quarter's average of 8.90 minutes. The increase in staffing alongside shift, training pattern and management changes is anticipated to reduce the call abandonment rate over time. In the reporting period there have been days when the target abandonment rate of 16% has been reached for the first time ever.

The Action Fraud confirmation survey looks at call handler knowledge, victim satisfaction with the service provided by the contact centre advisor, and the speed of answer. Feedback to this survey in Q1 indicates that satisfaction with the telephone reporting service remains stable and within target at 96%. This is a slight improvement on Q1 of FY 22/23 which saw a satisfaction rate of 95%. Overall satisfaction levels in this area remain high over the long term.

Online Reporting Service – Action Fraud are unable to make any changes to the current website, however a new reporting tool is currently in development and should launch early next year. It is anticipated that the new reporting system will bring online satisfaction in line with telephone satisfaction. In the short term, new facilities such as a webchat and chat bot have been added, improving victim satisfaction through the provision of support and guidance, assisting the victim through the self-reporting process. This increases the capacity of the advisors, enabling them to answer more calls and give more time to supporting vulnerable callers.

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 reduce the level of repeat victimisation after NECVCU contact.
- D. To ensure victims feel safer and more confident after NECVCU contact, with reduced emotional harm and improved sense of safety.
- E. To improve consistency of victim support across all police forces.



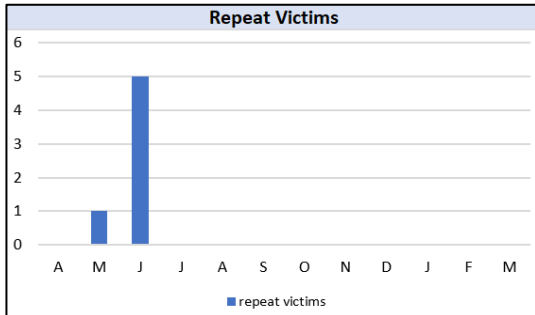
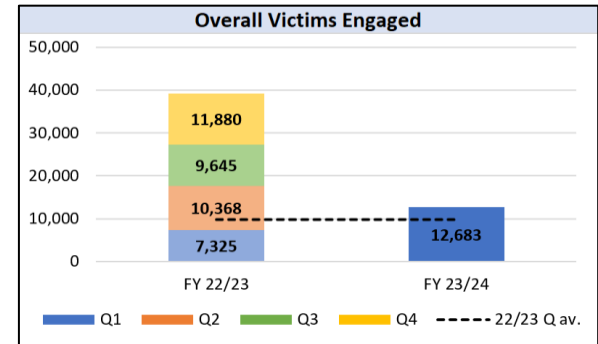
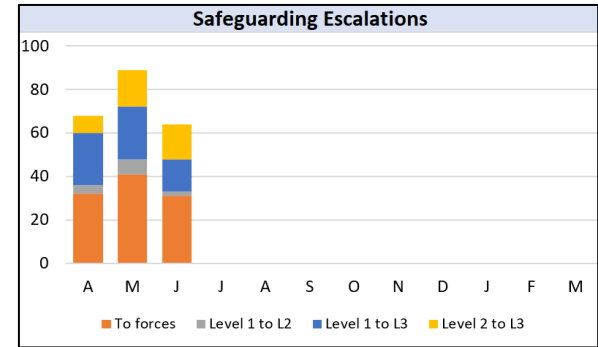
The **National Economic Crime Victim Care Unit** (NECVCU) supports forces at a local level, delivering care to victims of fraud and cyber-crime, allowing for a consistent and national standard of care and support.

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.

Repeat Victims – In Q1 the definition of a repeat victim became “a second or subsequent report by a victim of fraud who has had previous contact with NECVCU within a rolling 12-month period” whereas before there was no time limit. During the period there were 6 victims identified as repeat victims, down from the 2022/23 quarterly average of 26. In Q1 both services engaged with a total of 12,683 victims, meaning the 6 repeat victims represent 0.05% of victim contacts.

Victims feel safer – A victim survey has been launched, which measures whether victims feel safer and more confident after contact with an Advocate. Results are expected to begin to be available from Q2.

Consistent Support – The NECVCU now supports **41** forces in England and Wales at level 1 and following a significant staff uplift in May, provides **35** forces with an additional service at level 2 (formerly 6 forces), with talks to onboard more in the future. Escalations to provide additional service(s) to support vulnerable victims following interaction with NECVCU has remained relatively consistent in the period.



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 vulnerable person alert within 7 days.
- G. To review and respond to all allegations of fraud that meet 'highly likely' or 'likely vulnerable' on the solvability matrix, within 28 days.
- H. To provide an NFIB outcome to all victims, within 28 days.



Vulnerable Person Alerts – To identify potentially vulnerable victims, searches are run on all reports of fraud, looking for under 18s, and agreed 'risky words' which highlight a vulnerability risk for the victim – such as suicide, mental health, or threats to life.

In Q1 the search found 2,202 reports that came from vulnerable victims. Over the quarter, 84% of alerts were sent within the target of 72 hours, with a high of 99% in May. 100% of alerts were sent to forces for victim support within 7 days of the report being downloaded to the system

Priority Allegations – The process for prioritising which reports to review was developed in 2022. Rather than monetary thresholds, fraud reports are now assessed against a number of criteria to establish a 'solvability' score. Those 'highly likely' and 'likely' to be solved are prioritised for review.

During Q1, 31% of 'highly likely' and 41% of 'likely vulnerable' reports were reviewed within 28 days of reporting. During the quarter the overall volume of disseminations rose from 2,622 in April, to 4,257 in June.

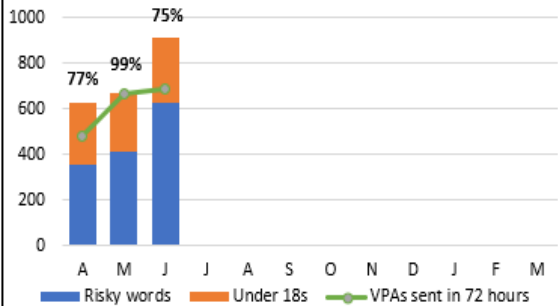
Victim Contact regarding Outcomes

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

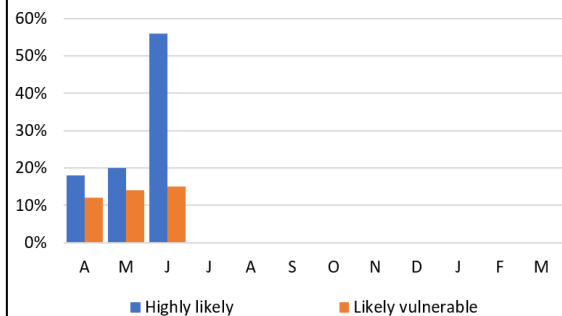
The NFIB has multiple advice letters, tailored to each fraud type, which are emailed to victims on a weekly basis. This service is known as 'Send in Blue'. In August 2021, this process was automated, and the success rate went from a low of 59% in June to an average of 99.69% for the rest of 2021/22.

In Q1 23/24, the success rate of Send in Blue was also 100%.

Vulnerable Person Alerts sent within 72 hours



Priority Allegations Reviewed within 28 Days

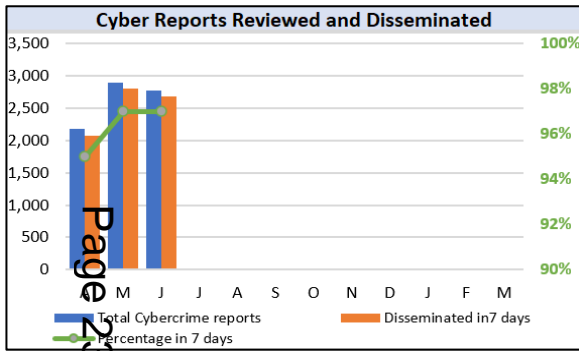


Outcome 1: Supporting and Safeguarding Victims.

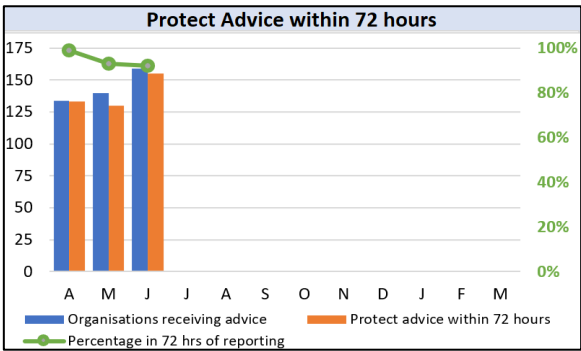
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:

- I. To review and disseminate all Action Fraud reports classified with an NFIB Cybercrime code, within 7 days of report creation.
- J. To respond to all live cybercrime reports, within 2 hours of reporting.
- K. All businesses reporting cyber enabled crime to receive Protect advice within 72 hours of receipt by the Protect Team.

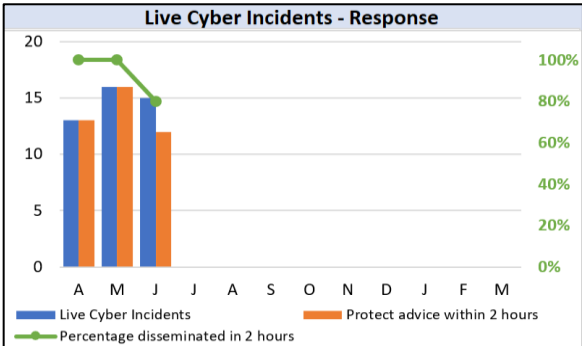


Live Cyber Incidents – 44 live cyber incidents were recorded in Q1, and in April and May each one was reviewed, and a response sent within 2 hours. In June, for the first time in over a year, performance fell to 80%. This is due to two reports being received out of hours within minutes of each other, meaning that with one on-call crime reviewer there was a 7-minute delay to the second report being reviewed and disseminated. The majority of reports are reviewed and disseminated in less than 60 minutes.



Cyber Reports – In Q1, 7,848 reports were classified with a Cybercrime code, up 22.5% from the previous quarter.

Of these, 100% were disseminated for Protect or Pursue activity, 96% within the target 7-day period. Performance improved from 95% to 97% throughout the quarter.



Protect Advice – NFIB Business Protect provided protect advice to 433 organisations during Q1, up 15% from the previous quarter. 95% (418) of organisations received the advice within 72 hours of reporting to Action Fraud. This measure may have been affected by the high number of bank holidays within the reporting period.



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:

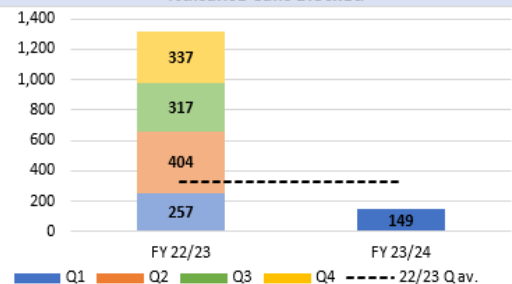
L. To help victims of fraud to prevent or recover losses through information sharing with the banking sector and support from victim care.



The **NLF Victim Care Unit** is a unique team, which acts as a conduit between NLF Fraud Ops Investigations and their victims of fraud. NLF VCU ensure that the Victims Code Of Practice is complied with and address the welfare needs of victims by triaging out to support services. They also play a part in the Protect strand of the 4P plan by proactively offering prevention advice to stop revictimization, also disrupting OCG activity.

NLF VCU have an ongoing partnership with Truecaller who install call blocking devices for victims who receive high volumes of fraudulent calls. Volumes dropped in Q1 due to two units falling dormant, but a further two were issued during the quarter.

Nuisance Calls Blocked

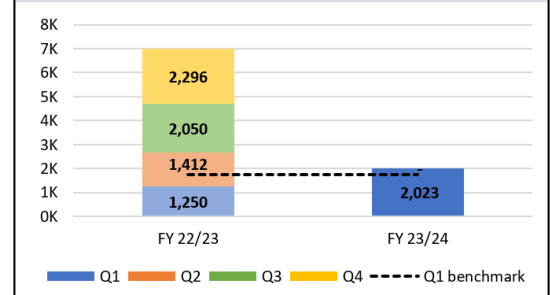


Project RECALL is an initiative to alert banks to accounts used in fraud. The process continues to function correctly, with the technical issues seen in 2022/23 resolved. This has resulted in an emerging baseline of just over 2,000 alerts being sent out each quarter with a value of £7-8 million. Overall alerts continue to be lower than the same period for 2021/22, however, the value of the alerts is higher. This is likely due to fraud reporting drawing closer to pre pandemic levels, with lower overall reporting but higher losses per report. With RECALL working correctly, volumes of alerts should continue to mirror trends in overall fraud reporting.

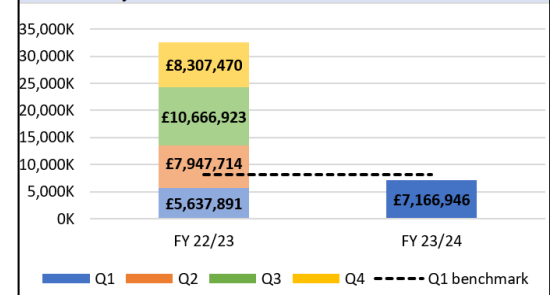
This quarter 2,023 account alerts were sent to banks, down 11% from Q4 22/23 (-273), however, this is a 61% improvement on Q1 22/23 when there were several technical issues. The value of Q1 alerts also fell slightly from £8,307,470 to £7,166,946. The system for banks to confirm the value of repatriated funds is not automated, and although the banks were proactively asked for feedback none responded in Q1.

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.

Project RECALL - No. Account Alerts Sent to Banks



Project RECALL - Value of Alerts sent to Banks

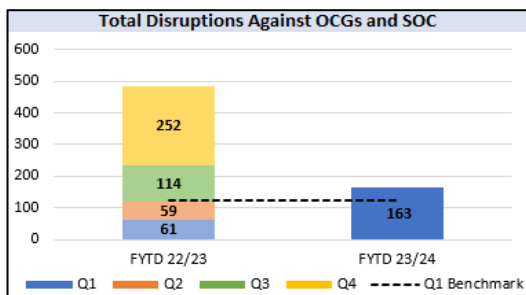
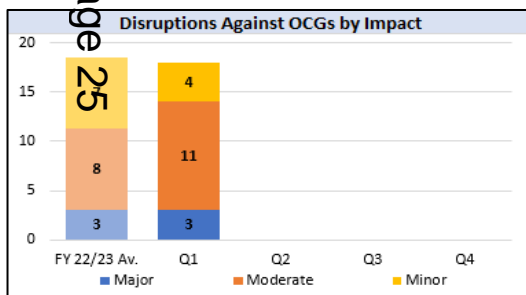
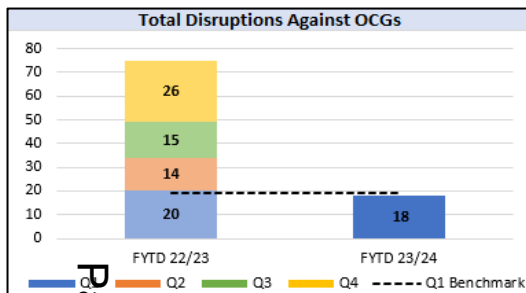


Outcome 2: Disrupt Fraudsters.

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 National Lead Force disruptions against Organised Crime Groups and Strategic Vulnerabilities.
- B. To increase the proportion of Major and Moderate disruptions.



There are currently 77 mapped **Organised Crime Groups (OCGs)** under investigation by National Lead Force teams. Four new OCGs were mapped in the quarter, and three were archived.

There were **18 disruptions** claimed against NLF OCGs in Q1, which is a 34% decrease compared to the 26 in Q4, although it is in line with the quarterly average from 2022/23. A Major disruption represents the OCG being fully dismantled or impacted at a key player level. There have been 3 major disruptions for Q1, and 11 moderate. There were an additional 145 disruptions against Serious Organised Crime strategic vulnerabilities throughout the period.

Activity against OCGs is not consistent and depends on a number of factors, including resources, capacity, and criminal activity. It is worth noting that approximately 35 of the active operations are Tier 4 investigations, meaning they are **awaiting court results** and/or are in their final stages before being archived. This means no further operational activity is planned against them and the only disruption left to claim is a Major once sentences are delivered. There have been many adjourned NLF cases in the last year, mostly due to Covid backlogs and barrister strikes.

Notable Major Disruptions

The **Fraud Ops** team secured a 14-year prison sentence for a criminal who ran a Ponzi-style investment scam worth over £70m. The suspect offered over 300 victims returns of 60% on foreign exchange markets. The suspect absconded part way through his trial and his whereabouts are still unknown. In his absence he was found guilty of 7 counts of fraud by false representation, fraudulent trading and money laundering.

Three suspects in a **PIPCU** investigation were convicted and sentenced to suspended sentences and unpaid work. Following the investigation evidence has been seen that their shops selling counterfeit goods have closed, and they now have legitimate employment.

The organisers of an **IFED** OCG were given a caution or served Cease and Desist orders. One nominal agreed to pay back the circa £7k he fraudulently took from Aviva.

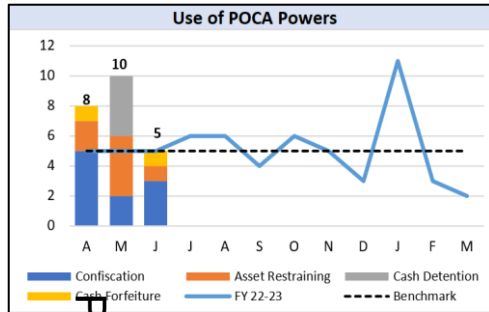


Outcome 2: Disrupt Fraudsters.

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.

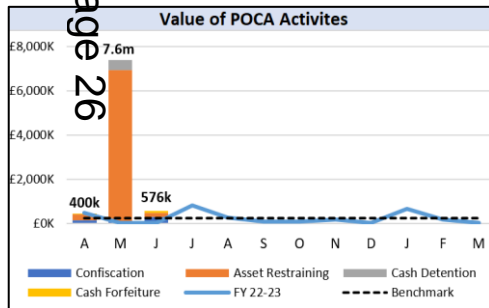
Success Measures:

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



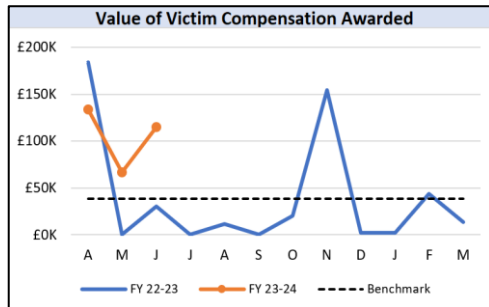
Use of POCA Powers

In Q1, Operational Fraud teams and Funded Units carried out 23 POCA activities. This is above the 2022/23 quarterly average of 15 and the Q4 total of 16. Most of the activity focused on confiscations (10) and asset restraining orders (7). The greatest value came in May, with three asset restraints carried out by PIPCU totalling £6.75 million. Additionally, the teams worked to ensure that Courts awarded 8 victims £315,295 compensation, which is above the 2022/23 benchmark.



Seizure of Cryptocurrency

PIPCU completed their first confiscation of cryptocurrency this quarter. The case involved a hacker who infiltrated numerous high profile artists' personal accounts, to steal items including unreleased songs and sell them for cryptocurrency. Working with the UK Digital Currency Exchange PIPCU officers were able to freeze the digital currency. Following conviction, the court ordered the confiscation order of 2.64522195 BTC which was transferred to fiat currency of £59,935.



Notable POCA Activities

This quarter saw PIPCU's highest POCA seizures, as a result of early restraints being obtained on all assets connected to suspects in two cases. The first is an investigation into the sale of counterfeit goods which are detrimental to public health, by a husband and wife who arrived in the UK in 2021 on a spousal visa. The suspected benefit figure could run into £6m with a current restraint order £1.03m. The subjects have used 30 different names resulting in 138 bank accounts so far identified. The second case is the investigation into illegal IPTV streaming involving the top tier, which includes a father and son and an in-law. Similarly, the suspected benefit figure runs over £4m with a restraint order of £1.68m. There are 86 accounts so far identified.

In May, IFED obtained an account freezing order of £459,762 regarding a company who had incepted 390 life/critical illness insurance policies using false details, and fraudulently claimed over £1.07m of commission. The OIC obtained the AFO to freeze the accounts before the funds could be dissipated. The sole director and owner of the company and had used the funds to purchase a holiday wedding in Cancun, a new BMW, and a Rolex Watch from his business account which amounts to money laundering.



Outcome 2: Disrupt Fraudsters.

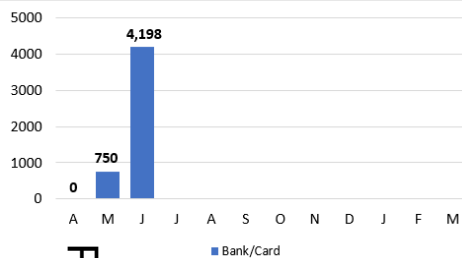
NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

Success Measures:

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



Number of Disruptions to Cards and Bank Accounts



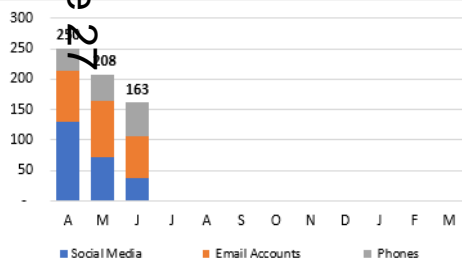
Notable Disruptions

DCPCU saw high numbers of bank account disruptions due to two investigations into account takeovers by organised crime groups. A suspect who is currently in prison was interviewed and revealed that a mobile phone in their possession during the offending period was still in his property. The device was seized and examined revealing thousands of sets of compromised account details, which were shared with UK Finance to safeguard accounts and identify offending. In another investigation, two bank insider suspects were identified, arrested and interviewed. Their devices were seized and compromised account data found. This was shared with UK Finance to protect the accounts.

During Q1, a total of 8,087 disruptions to technological enablers were recorded, lower than the Q4 22/23 quarterly average of 20,308, but almost double than the Q1 22/23 total of 4,259.

Volumes of disruptions fluctuate throughout the year according to operational priorities and intensifications.

Number of Disruptions to Other Technological Enablers



NFIB's Prevention and Disruption team (P&D) identified and disrupted 20 suspicious email addresses set up by a trading company in a sophisticated investment fraud where adverts for investment training were placed on social media sites. Tuition included fake videos in the name of money expert Martin Lewis to legitimise the company. On signing up, victims were subjected to high pressure sales tactics to invest funds for trading purposes. At the point of final withdrawal, contact would be withdrawn, and funds withheld. Reported losses at point of disruption were £2.6mil. P&D also assisted Sir James Dyson with a case of multiple websites set up to commit crypto based investment fraud. The company used social media to attract investors, attaching fake Times news articles using his name to recommend them. P&D were able to take these sites down when Sir Dyson's legal team were unable to.

City of London Police and National Cyber Security Centre (NCSC) Suspicious Email Reporting Service (SERS) and Takedowns

The public are sent large volumes of scam messages every day, many of which will be blocked by spam filters or otherwise ignored. NCSC and CoLP receive reporting of suspicious emails from the public via SERS, which launched on 21st April 2020. As of 30th June 2023, the number of reports received stands at more than 21,981,000 with the removal of more than 133,000 scams across 242,600 URLs.

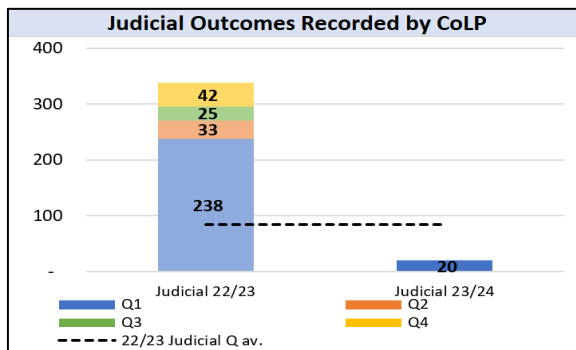
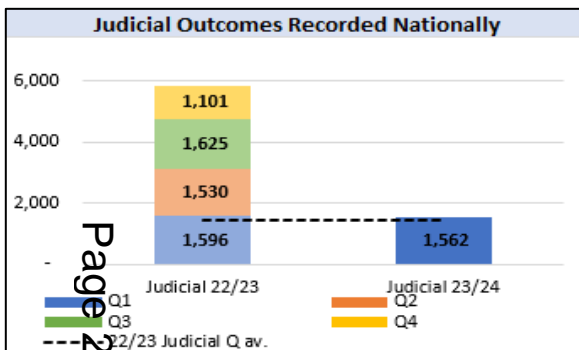
In Q1 there were over 29,230 suspicious emails reported per day to NCSC and CoLP, in addition to around 888 cyber-enabled crimes reported by victims to Action Fraud.

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



Nationally, Q1 2023/24 judicial outcomes are broadly in line with the comparative period for the prior year. Significant contributions were made by Merseyside, Northumbria and Lancashire, who collectively contributed 250 judicial outcomes (16% nationally). This can be attributed to continued engagement by the NCO in its engagement and holding forces to account - not only through Regional Strategic Governance Groups, but also through the Economic Crime Policing Board and the monthly performance reports that all forces now receive following the HMICFRS Time to Choose recommendations.

CoLP Judicial outcomes are down by 218 or 92% in Q1 2023/24 compared to the prior year. This is primarily due to the Fraud teams undertaking a sweeping exercise of old Judicial outcomes last year. They finalised 186 in total through this process, and in addition one large NLF operation yielded 23 Judicial outcomes in this period.

The total outcomes reported in a 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 many outcomes, potentially bringing closure to multiple 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 23/24 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 provided their return each month. The National Coordinators Office (NCO) continue to engage with forces to ensure compliance is maintained.



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.

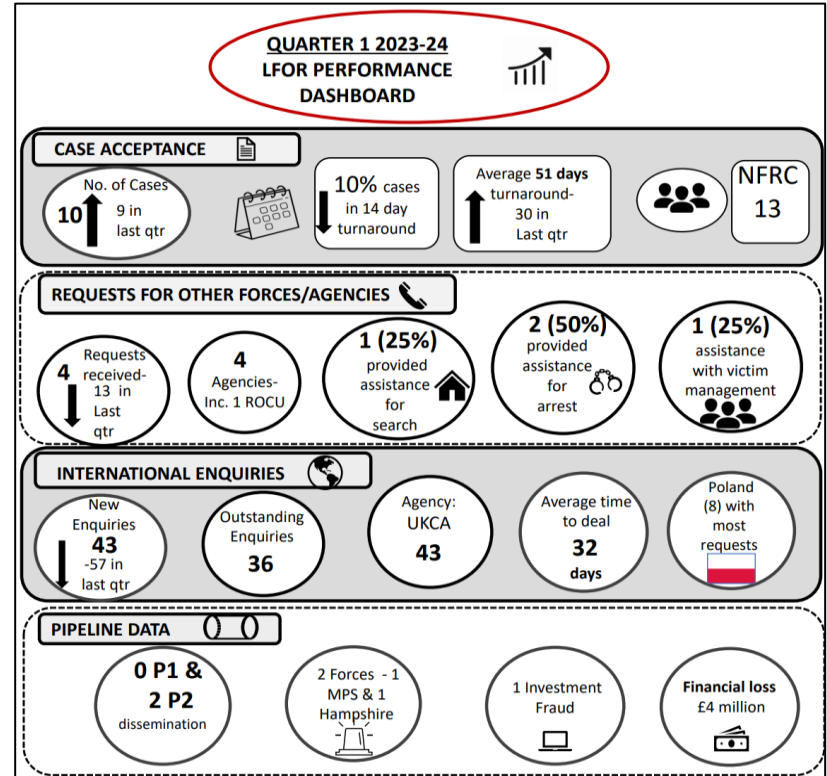
National and International Coordination and Assistance

LFOR assisted other Forces and Regions with **4 requests for assistance** during Q1 2023/24. The requests were for arrests, warrants to be executed, supporting premises searches, gathering of evidence, as well as victim management. This is a key role of LFOR who 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.

LFOR received and developed **10 cases** that were subject of **Case Acceptance Plans** for consideration by NLF Operations. This compares to 9 cases the previous quarter.

There have also been **43 International requests for assistance** from Foreign Law Enforcement Agencies. These are managed within LFOR, and during this quarter the highest number of requests were again from Poland. The average time for completion for Q1 was 32 days which is well within the 90-day target.

LFOR coordinate the activity of the regional **Proactive Economic Crime Teams** and monitor their performance against agreed KPIs. During Q1 the PECT carried out 49 arrests, 25 voluntary interview and 170 alternat outcomes. They also submitted 196 intelligence reports and seized assets valued at £625,372.00 . The PECT were all involved in Op Dupers targeting Courier Fraud in May.



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.
- B. To increase the reach of Social Media posts (impressions).



Across the various teams engaging on social media, the number of confirmed posts (457) and related impressions (3.2 million) rose from Q4 22/23. Action Fraud has engaged with new platforms, with 4.5k followers on Instagram, and is now active and verified on the Threads social media platform. The NFIB Protect Team have had issues providing social media reach and impression data, so their campaign details will be discussed on the next slide.

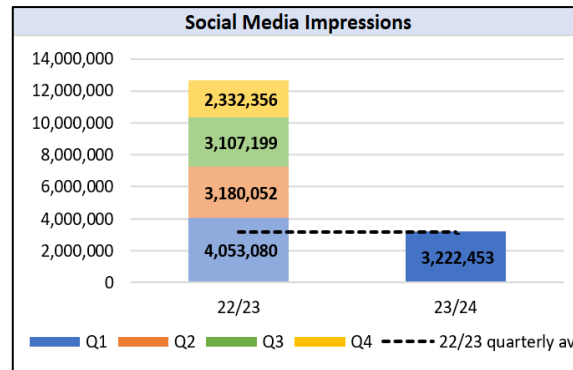
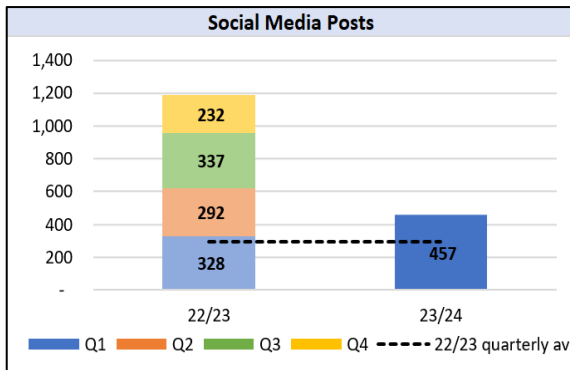
During the quarter, the Media Team oversaw 17 press releases and 2 interviews. Compared to the previous quarter, this represents a decrease for interviews, however a significant increase for press releases. The interviews included a filmed section for BBC One's Caught Red Handed (to air in August) and background for an article on luxury counterfeit goods with The Guardian. Press releases received coverage in local, national and trade media and included the rise in opportunistic insurance fraud, an IPTV sentencing, a warrant executed with Amazon, a fraudulent pet insurance sentencing, and a suspect going on the run after being sentenced. A press release was also issued announcing the new suppliers appointed for Action Fraud.

Notable Social Media Campaigns

IFED issued press releases on social media regarding a sentencing about fraudulent income protection policies, and to promote the repayment of a confiscation order. They also supported Insurance Fraud Bureau campaigns on crash for cash moped scams and opportunistic insurance fraud.

The **NLF Operational Teams** posted further messaging regarding Hajj fraud, supported the Action Fraud ticket fraud campaign, and launched a Courier Fraud campaign with a press release around over 70s being disproportionately targeted.

Press releases were issued by **PIPCU** following three people sentenced for running an illicit counterfeit goods shop in Manchester with over £1m worth of fake designer goods seized. Also, after PIPCU secured a confiscation order against a hacker who was jailed in October 2022.



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.



NLF: Romance Fraud Campaign

June saw the end of the 6-month NLF romance fraud campaign in partnership with CrimeStoppers. This used established CrimeStoppers platforms to deliver Protect messaging to communities and organisations. The products were sent to 74 agencies including Neighbourhood Watch, adult safeguarding services and safer community partnerships. The campaign received 8.1 million impressions, media interest and was promoted by the On-line Dating Association.

The content and graphical representation showing the true meaning behind fraudsters' messages was well received and shared across many partner organisations with the social media posts generating a wide range of responses.

The total audience reach is approximately 92.3 million and the relationship with CrimeStoppers has proven to be valuable in supporting national Protect messaging to assist with the safeguarding of vulnerable victims. DCI Parish has approached the NECC to discuss funding opportunities for this year to support other fraud related initiatives.

LFOR: Courier Fraud

Op Dupers was a proactive operation to target courier fraudsters and disrupt them from committing fraud against vulnerable and predominantly elderly victims. The LFOR led operation was undertaken with support from the NECC, NFIB, IDT, ROCUs, and local forces including the Met.

The participation and engagement was excellent and during the intensification, a number of successful outcomes and significant intelligence were identified.

NFIB Protect and Action Fraud

During the 21/22 reporting period, Action Fraud received 6,457 reports, amounting to over £15m lost to **Holiday Fraud**. During May, the NFIB Protect team delivered a social media campaign to raise awareness of this threat. This campaign built on behaviours delivered during the online shopping/Cyber Aware campaign and aligned to the new fraud/cyber communications toolkit. The campaign reached an estimated 6.4m individuals, achieving over 22.8m impressions.

During June, the Protect network delivered its annual **phishing awareness** campaign. The campaign reached 6.1m individuals, achieving over 14.1m impressions. The campaign aimed to raise awareness of reporting suspicious emails to report@phishing.gov.uk and reporting suspicious text messages to 7726. As of June 2023, the number of reports received stands at 21m, with 133k scams being removed across 242,600 URLs. 18k scams have been removed as part of the 7726 service.



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

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.
- B. To maintain delegate satisfaction levels at 90% or above.

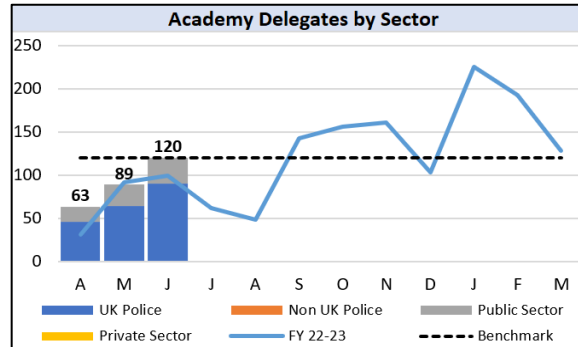


Training Courses

The ECCA delivered 22 training courses in Q1. Although this is a decrease of 50% from Q4 22/23 it is a 15% increase from the 19 courses in Q1 of the previous year. Training levels are following the expected seasonal adjustment, as bookings are affected by budgets and bank holidays in Q1.

The number of delegates, 272, represents an increase of 23% from the same period of the previous year (221). This represents an ongoing year on year increase in the number of both courses and delegates.

This quarter, 75% of delegates were from UK policing, with remainder from the private sector.

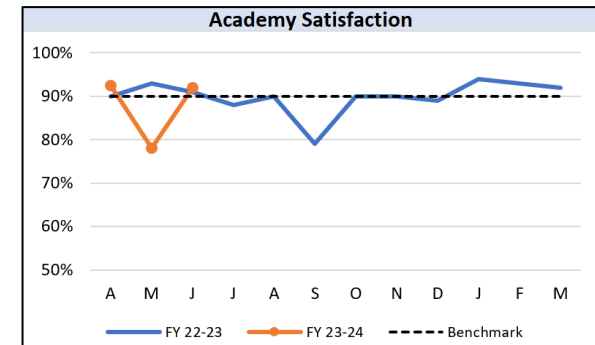
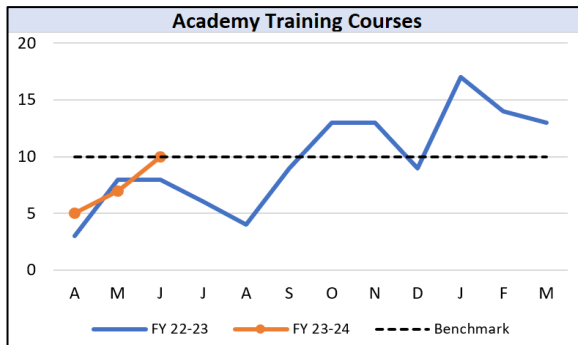


Satisfaction for the quarter averaged at 88% despite a drop to 78% in May. This was due to a free SFI course that was held externally. Several delegates felt it was not relevant to their role, and the facilities were unsuitable. Only 51% of feedback forms were returned during the quarter. This will be addressed by the training admin team for future courses.

Currently, the Academy asks for feedback on the course itself. In the future, a strategy will be instigated to contact delegates' managers following the course, to understand if the lessons learned have been implemented, and from both their perspectives, how the course has assisted them in their investigations.

The Academy delivered a Victim Care course for new Advocates in the NECVCU expansion, ensuring NLF staff have appropriate skills. Throughout Q1, other training was delivered to partner organisations, including Demystifying Cyber Crime to the Cabinet Office, and FIFC and SFI courses to SEROUC officers.

The Academy delivered a bespoke Introduction to Fraud course specifically designed for the FCA and the NCA were given a Bribery course. Feedback from both has been positive and early indication is they will request additional courses.



Page 32

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.



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. In Q1 2023/24:

IFED worked with CPS lawyers and a FTSE 100 insurer to obtain an Account Freezing Order for £459k under POCA.

PIPCU continued its successful collaborations with World Intellectual Property Organization and Europol to disrupt pirate and copyright-infringing websites.

In May **PIPCU** worked with Sky to utilise a new tactic to disrupt illegal TV, utilising Sky expert knowledge.

The **Intelligence Development Team**, financed by Lloyds Banking Group used licenced demographic segmentation data to identify chronic hotspots of victimisation and forecast potential victimisation by location. Greater Manchester Police found that using the method devised reduced victim losses to romance fraud in hotspots by up to 100% over six months.

Spotlight on DCPCU and Lloyds Banking Group

Lloyds Banking Group has joined forces with the DCPCU to launch the industry's first pilot scheme using proceeds of crime to fund a national fraud fighting programme. The 'frozen' cash – which is money captured from fraudsters by the bank's specialist mule-hunting team – has been invested in several projects to tackle fraud.

One of these is expanding the DCPCU by funding a new specialist team to track down criminals through cyber investigations, which can lead to disrupting other illegal activity often associated with fraud such as drugs and people trafficking.

Research conducted to support this partnership revealed that a criminal's traditional weakness, 'cashing out' the crime, had become a strength as they are using cryptocurrency to disguise their transactions from financial institutions. Research also revealed that there were no pathways to proactively identify key threat actors. The DCPCU utilised the funding to develop an 'intensive cyber training pathway', exploiting the blockchain and identifying 'real world' touch points for criminals exploiting the perceived anonymity of cryptocurrency. These newly trained investigators were enabled to develop 3 key workstreams.

- Target criminals purchasing software to bypass financial institutions' authentications.
- Target criminals who were trading in stolen data purchased on the 'dark web'.
- Identify and target prolific fraudsters on encrypted messaging platforms.

This partnership enabled the development of a thorough digital strategy, including training staff to search for compromised customer data on devices seized from suspects and sharing it with industry to protect accounts and prevent further offending. In 2022 this new workstream demonstrated outstanding performance. The targets agreed with stakeholders were for the team to annually achieve £14.5m of savings to industry and seize £0.3m from the hands of criminals. As a result of this project, in 2022 (the projects first year), the development of these investigations enabled the new team to **arrest 26 nominals**, achieve **5 convictions**, **seize £0.89m** from criminals, and **save industry an estimated £35.3m** by protecting thousands of customer accounts. As a result of this successful partnership the DCPCU are looking at incorporating their new team and working practices into their standard operating model.

Public Sector Online Service Providers
Law Enforcement
Trade Groups
Brands
Insurance
Banking & Financial
Third Party Service providers
Information Technology

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.



Establishment of a new Fraud Policing Network (PURSUE):

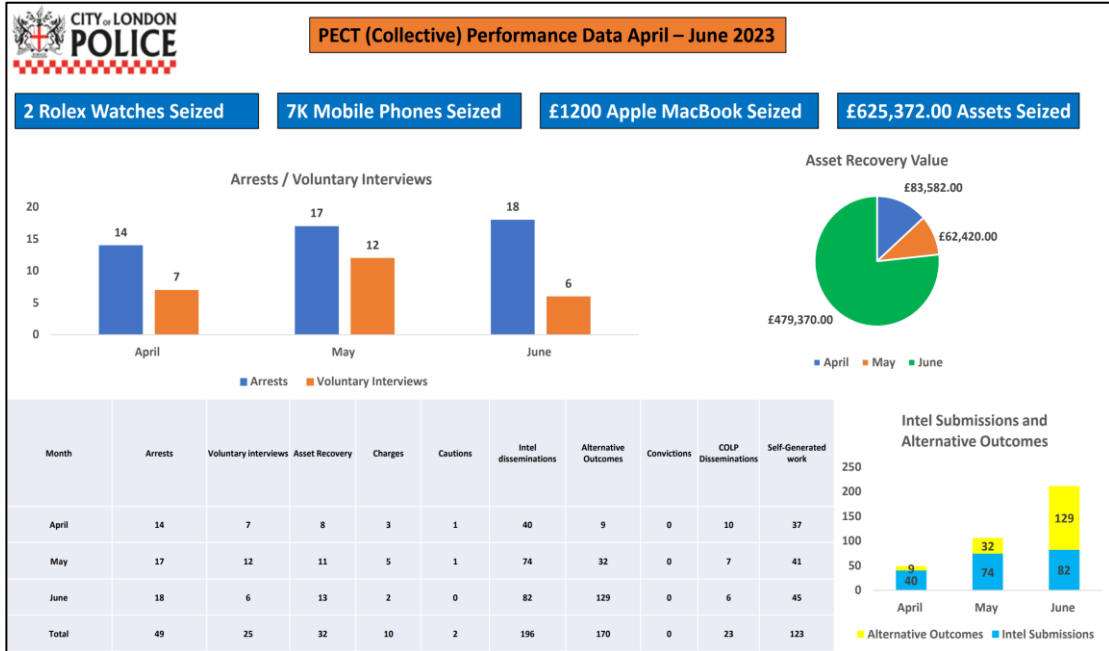
- There are 9 Regional Proactive Economic Crime Teams (PECTs) in place and enlargement of the London response (MPS and CoLP) is being implemented with DI already in post, and 2 DCs from CoLP, and 1 DS and 3 DC from the MPS.
- By the end of June 2023, 124 regional posts were in place across the network, representing 72% of the target by FYE 2023/24 (172 posts) achieved. This is across both the Police Uplift Programme and HMG Spending Review investment funding.
- Assessment of PECT operational performance is regularly monitored and a dashboard for regional accountability has been devised.
- The growth in investigative capacity in CoLP NLF Fraud Operations has resulted in 8 new Police Staff Investigators and a PSI Supervisor in place.
- 4 CoLP leadership posts are being recruited in 2023/24. A Communications lead is in place and a DI PECT Coordinator, Performance Lead and Intelligence Lead are being recruited.

Notable operational examples include:

ERSON Enforcement at two properties culminating in recovery of £15k counterfeit and a large quantity of drugs. Enforcement undertaken in Birmingham of three suspects culminating in the charge and subsequent remand of two linked to a series of circa £40k CF offences. Multiple devices recovered, and a third suspect bailed.






TARIAN Dyfed Powys Police were subject to a number of courier fraud incidents. Charter work was conducted by Tarian PECT on the VC number and call data was obtained. On analysing the data returned, another possible victim was identified due to the amount of contact with the VC number. Dyfed Powys Economic Crime Team were then able to carry out an immediate response, which showed the offence was in process and prevented a loss of approximately £15,000.

NWROCU Postal fraud. A warrant was executed at an address in St Helens. Two Indian nationals were arrested at the address. Cash seizure and AFOs of approximately £10,000. No comment interviews and bailed.



Appendix A - Performance Assessment Criteria

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 assessment for the relevant measure. These have been identified based on the data available, and whether the data is increasing or decreasing within the required tolerance level.

Success Measure Performance Assessment	
Page 35 	A green upwards arrow suggests improvement in the direction of travel.
	A green arrow pointing right is used for consistent performance at 100%.
	A green arrow pointing down means a decreasing trend which is positive.
	Amber means there has been limited increases or decreases within tolerance level.
	A red downward arrow suggests a decrease in performance.



This page is intentionally left blank

Committee: Economic and Cyber Crime Committee	Dated: 8 September 2023
Subject: National Lead Force and Cyber Update	Public
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1,10, 12
Does this proposal require extra revenue and/or capital spending?	N
If so, how much?	NA
What is the source of Funding?	NA
Has this Funding Source been agreed with the Chamberlain's Department?	NA
Report of: Commissioner of Police Pol 87-23	For Information
Report author: Kevin Ives, Staff Officer to AC O'Doherty	

SUMMARY

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

- Some cross border work from the operational units
- One of the largest and most complex Fraud Investigations to take place and outcomes achieved
- Effective communications campaigns

Recommendation(s)

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

MAIN REPORT

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.

Action Fraud (AF/) National Fraud Intelligence Bureau (NFIB) Action Fraud published an alert on the 18th August via social media and the messaging service after receiving 468 reports in two weeks relating to fake emails purporting to be from ASDA. The emails claim that the recipient has won a 'free' air fryer and provides a link the recipient should follow to claim their prize. The links in the emails lead to malicious websites designed to steal personal and financial information. This is an excellent example of a very fast response to an emerging problem.

National Economic Crime Victim Care Unit (NECVCU)

In this period there has been national media coverage of the completion of NECVCU's expansion programme; the unit now provides a service to all forces in England and Wales. The media story was headed up by AC O'Doherty and received further promotion from the Home Office's Economic Crime Policy team.

Fraud and Cyber Crime Reporting and Analysis System (FCCRAS)

The outline plan for system interoperability has been agreed. This will see the new system connected to PND(Police National Database for intelligence) benefitting UK policing and partner Law Enforcement Agencies. There will also be new connections with public and private sector counter-fraud databases in order to STOP and BLOCK fraud and cybercrime.

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.

Police Intellectual Property Crime Unit (PIPCU)

Italian authorities requested PIPCU attendance at EuroPol to discuss Operation Cassandra. This ongoing operation involves a Senegalese OCG based in Bristol, who are at the centre of importing counterfeit clothing / watches / handbags into the UK from China, which are then exported to Italy and Spain. The meeting covered links between the two cases and the best way of sharing information and evidence and sharing information on connected cases in the future via Siena to prevent / disrupt this activity on an international scale with disruptive seizures and also some pursue activity. A separate report on more PIPCU activity is on the agenda.

Insurance Fraud Investigation Department (IFED)

On 19 July 2023, DCI IFED presented National Tactical Guidance on the use of Cease & Desist for Fraud and Economic Crime to the Economic Crime Partnership Board, chaired by the North West Regional Organised Crime Unit (ROCU). In one week in July alone IFED officers served 6 cease and desist notices across the UK. This is a tactic initially designed by PIPCU which is now slowly being picked up across the UK as a major disruption tool for lower level crime.

Dedicated Cheque and Payment Crime Unit (DCPCU)

Officers attended The Hague to develop a joint investigation team with the authorities from Finland and Switzerland in relation to a UK based global threat actor who is mass producing 'Phish kits' to fraudulently purport to be from various national / international financial organisations. The planned work will not only disrupt cross border crime but also help prevent further schemes from taking place by building and sharing knowledge.

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.

National Lead Force (NLF)

In June Operation Vanbrugh, one of the largest ever investigations into a 'ponzi' style fraud reached a successful conclusion after five years of investigation, the lead suspect was convicted of seven counts of fraud offences and on the 9 June 2023 he was sentenced to 14 years in prison, which reflects the huge harm caused to the hundreds of victims who lost life savings, houses and pensions whilst the suspect spent their money, on one occasion £2.5 million on his own wedding day. The total value of the fraud was £70million. The suspect fled court before the verdict and a live manhunt operation is now underway.

Asset recovery continues and the Force has participated in the recording of a podcast for a UK broadcaster.

Lead Force Operations Room (LFOR)

Great national co-ordination work on the 24 May LFOR assisted Northeast Regional Special Operations Unit with executing a warrant and arresting a suspect in relation to a courier style postal fraud. Op Duper, a National Courier Fraud intensification concluded on 19 May, but LFOR has continued to assist forces and regions this week with ongoing courier fraud investigations which had begun during the intensification.

Police Intellectual Property Crime Unit (PIPCU)

Operation Matthaus utilised resources from across the Force including Mounted, Tactical Support Group, COLP Cadets, MPS Police Neighbourhood team, Camden Trading Standards and stakeholders from the Anti-counterfeiting group in the search of two counterfeit shops; three arrests and seizure of £5 million in counterfeit goods. This area is very likely to see further major features in the future as counterfeiting has grown there, potentially in response to the PIPCU inspired shutdown of Cheetham Hill which has seen counterfeiters begin to be driven from that area.

Fraud Ops

Op Curry -Over the course of three years, offenders ran 'Digi Ex' – a company that cold-called potential investors to part with their cash in exchange for a fictitious cryptocurrency called Telecoin. From 2015 to 2017, a total of £509,599 was credited into Digi Ex accounts. The trial was very complex, with the defence attempting to discredit the investigation. The two defendants were found guilty and sentenced to 6 years and 6 ½ years, respectively. Both were disqualified as Directors for 8 years. This case is a great indication of how the teams are dealing with high-tec and modern fraud types.

Outcome 4: Raise Awareness and Prevent Crime.

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

National Fraud Intelligence Bureau (NFIB)

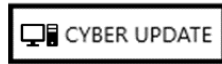
June saw the conclusion of the 6 month NLF romance fraud campaign, in partnership with CRIMESTOPPERS. Designed to deliver Protect messaging to a variety of communities and organisations. Messaging was sent to 74 individual agencies including Neighbourhood Watch, adult safeguarding services and safer community partnerships. The campaign received 6.7 million impressions and received media interest from various sources as well as communications promoted by the Online Dating Association (ODA).

Action Fraud

Action Fraud's annual holiday fraud campaign attracted positive coverage across local and national media outlets. There was also widespread coverage of Action Fraud's alert on ticket scams linked to the forthcoming European football finals.

On 7 July 2023, the Action Fraud / NECVCU / NFIB team hosted Anthony Browne MP, the government's new anti-fraud champion. This 'meet-the-team' input enabled Mr Browne to better understand the breadth of the three team's nationally significant work – and how this supports the government's National Fraud Strategy. Mr Browne showed a particular interest in efforts to prevent fraud and cybercrime, specifically the work CoLP delivers to STOP and BLOCK fraud through jointing working with banks,

TELCOs and social media platforms. After the event, Mr Browne tweeted a photograph of the visit (his time spent with the NECVCU team).



National Fraud Intelligence Bureau (NFIB)

There has been positive media coverage of the joint NFIB / National Cyber Security Centre (NCSC) Suspicious Email Reporting Service (SERS). Since April 2020, the service received 21 million reports and led to the removal of more than 235,000 malicious websites, 54,000 text message scams, and 7,726 suspicious texts, providing a huge victim service impact.

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.

Police Intellectual Property Crime Unit (PIPCU)

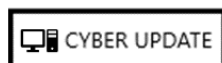
The unit hosted delegates from the International Anti-Counterfeiting Coalition (IACC) who are based in Washington, and Senior Officers from Homeland Security Investigations. The visit was designed to finalise plans for an international conference to be held in London between the 5 and 7 December this year. The Conference will be for 350 delegates from around the world and jointly hosted by IACC, US Homeland Security and CoLP (PIPCU). Formal plans are now being drafted.

National Co-Ordinator's office

In July the force engagement reviews were conducted with Cheshire Police, with reviews for Humberside, West Midlands and Yorkshire Police due on 08/08/23. This shows the continuous improvement work taking place led by City Police.

Economic and Cyber Crime Academy

The Home Office has made further contact with regards to the ECCA providing training to Mauritius Law Enforcement. The Australian Federal Police are scoping the viability of replicating the ECCA within Australia, and to explore potential joint working. It is likely an Australian delegate(s) will attend our Fraud Investigation Foundation Course, Specialist Fraud Investigator Programme and Accredited Counter Fraud Manager.



NPCC Cyber

On 3 July 2023, a presentation was given on Cybercrime and the future challenges especially around competing demands and the metaverse to the Judges at the Old Bailey at the request of the Sheriff Andrew Marsden.

On 4 July 2023, D/Supt Cyber presented to the Public Technology annual Cyber Security Conference on Cybercrime and the policing response and challenges.

In June the NPCC cyber team gathered all senior regional leads to present updates and have a two day workshop of the new operating model amongst other changes.

Committee(s): Economic and Cyber Crime Committee	Dated: 8 September 2023
Subject: Q1Cyber Griffin Performance Update 2023-24	Public
Which outcomes in the City Corporation’s Corporate Plan does this proposal aim to impact directly?	1- People are Safe and Feel Safe
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 88-23	For Information
Report author: Inspector Charlie Morrison, Cyber Griffin.	

SUMMARY

Cyber Griffin has continued its period of strong performance through Q1 and is currently significantly ahead of its local and national targets for the year. As encouragingly, the forecast for work looking ahead to Q2 is also very strong. It is expected the programme will continue to perform well through the autumn period of the year. The software used for one of Cyber Griffin’s services, the Cyber Capability Assessment, has been unusable due to platform migration work throughout this period. It is due to return in September. Work to complete a fully costed proposal for national work continues.

RECOMMENDATIONS

It is recommended that Members note the report

MAIN REPORT

INTRODUCTION

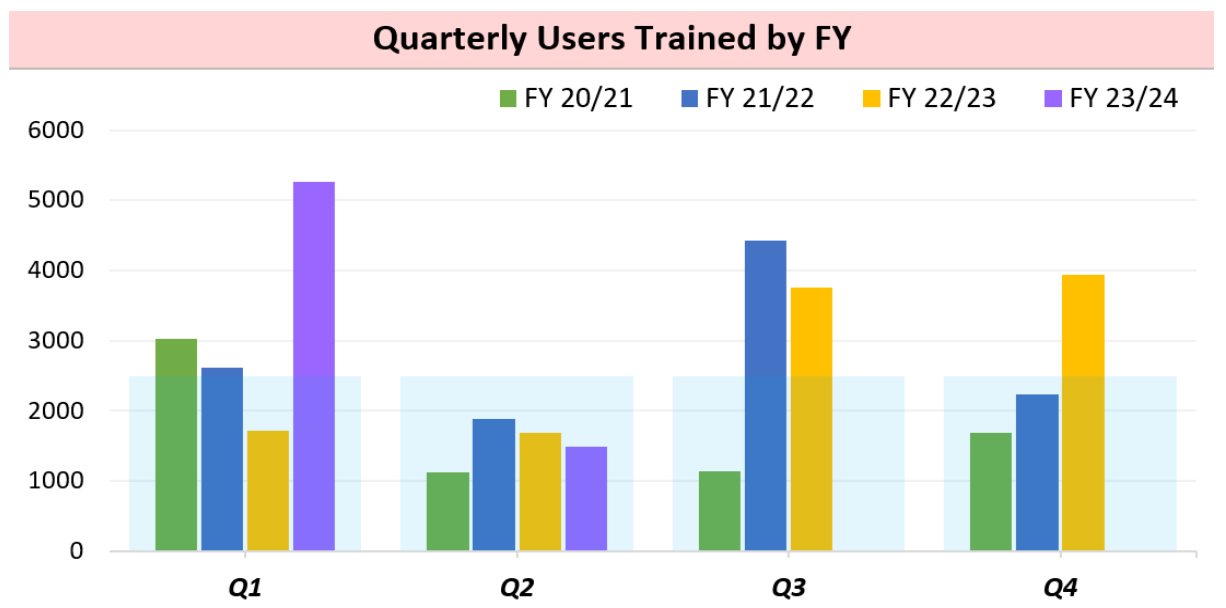
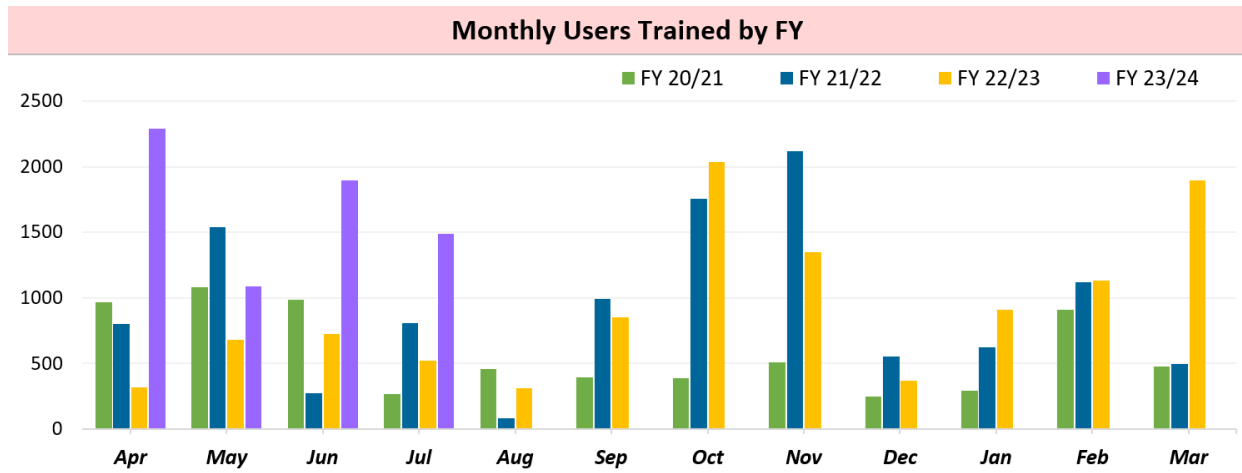
1. This report gives a brief update on the current position of the Cyber Griffin programme. For details of all Cyber Griffin services please visit: www.cybergriffin.police.uk

CURRENT PERFORMANCE POSITION

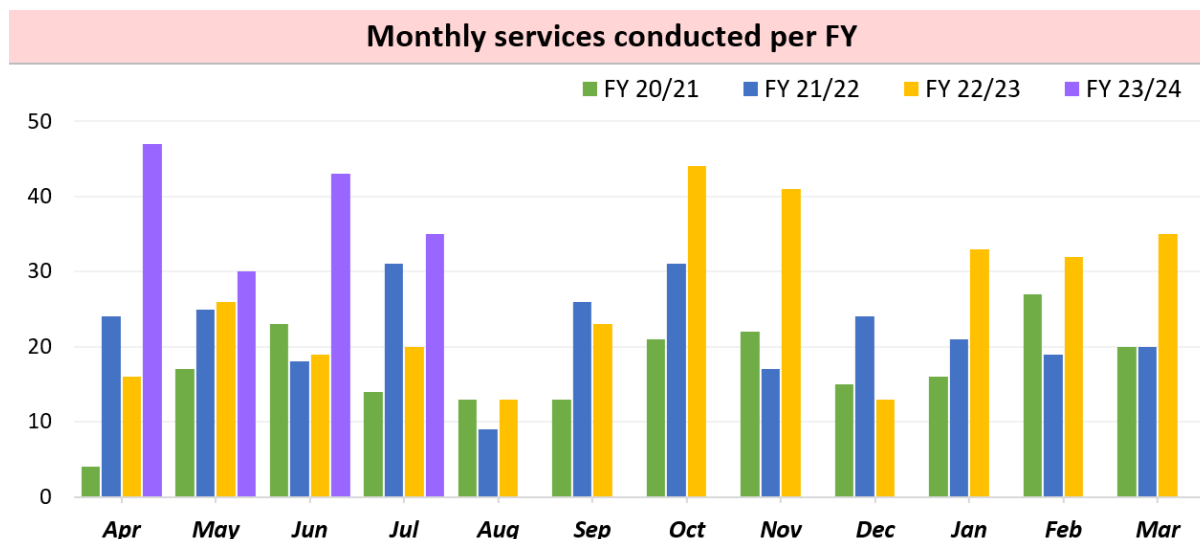
2. For the first time, Cyber Griffin has trained more than 5,000 people in a single quarter. Q1’s strong performance was driven by several positive factors. A growth in return bookings from long-term partners is visible in performance data

and the team's reliance on digital delivery has allowed services to be scaled to meet rising demand. The period also saw a very low level of unit abstraction combined with the team's release of a new case study focused on spear phishing attacks which has been extremely well received. It is also worth noting, that changes in counting figures have increased performance reporting but these account for less than 5% of the increase in performance observed.

Graphs showing Cyber Griffin's monthly and quarterly users trained compared with previous financial years



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



3. Regarding locally set targets, all are either on track to be met by the close of the financial year or ahead of target. In Q1, the programme trained 5,267 people (quarterly target of 2,500), conducted 120 services (quarterly target of 67) and partnered with 58 new client organisations (quarterly target of 36). In terms of Cyber Griffin’s performance goals for the financial year, the programme is currently significantly ahead of target in all areas.
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. Survey data also 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. This extra demand is manageable at present with existing resources.
5. Looking ahead at programme’s performance, data from previous years suggest that Q2 of the financial year will see a drop in performance which is typical for the summer months followed by the busiest period of the year, September onwards. Currently, Cyber Griffin’s work forecasting predicts the same trend will occur this year.
6. Cyber Griffin’s financial situation remains very positive. The programme has confirmed both the Corporation Business Levi and NPCC Cyber Crime Programme funding. Combined with the unit’s current funding, Cyber Griffin has stable long-term funding going forward.

7. During this quarter Cyber Griffin released the Baseline Briefing 4.0 which has revised our teaching of cyber threats to reflect trends seen in 2023. The programme also released a case study which takes attendees through a Cyber Crime Unit investigation of criminals engaged in spear phishing attacks. Both have been extremely well received. Cyber Griffin's new Incident Response Exercise which has been developed in partnership with Bristol University is now in its final testing stages. It is anticipated the exercise will be released in Q4.
8. Cyber Griffin have been unable to complete Cyber Capability Assessments this quarter due to the software supporting this service being unavailable while it is migrated to a new platform. The service is due to return at the end of Q2. A significant but manageable backlog of assessments will be worked through at that point.
9. The potential for Cyber Griffin to extend its work into the national PROTECT space continues to be considered. A fully costed detailed design has been submitted for senior officer consideration. This work has now been through several iterations and is close to completion.

CONCLUSION

10. Cyber Griffin continues to offer a very well-regarded and effective cyber security programme. Very positively, Cyber Griffin is significantly ahead of its performance targets for the year currently and forecasting suggests a further healthy period of performance in Q2. Software issues have caused a backlog of Cyber Capability Assessments which will start to relieve in September as the software becomes available again. Work to submit a fully costed proposal and detailed design for national PROTECT work continues. This work represents an excellent opportunity for future development.

Contact:

Charlie Morrison

Inspector

Cyber Griffin

City of London Police

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

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

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

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

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

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank

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

Document is Restricted

This page is intentionally left blank