Public Document Pack

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

Date: **FRIDAY, 25 NOVEMBER 2022**

Time: **9.00 am**

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

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

Enquiries: **Richard Holt**
Richard.Holt@cityoflondon.gov.uk

Accessing the virtual public meeting Members of the public can observe this public meeting by following the link:

https://youtu.be/X7pw3oWSIhA

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

John Barradell
Town Clerk and Chief Executive

AGENDA

Part 1 - Public Agenda

1. **APOLOGIES**

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

3. **MINUTES**
To agree the draft public minutes and non-public summary of the previous meeting of the Economic and Cyber Crime Committee held on the 3rd of October 2022.

For Decision
(Pages 5 - 10)

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

For Information
(Pages 11 - 12)

5. **ECONOMIC AND CYBER CRIME- COMMUNICATIONS AND STAKEHOLDER ENGAGEMENT UPDATE**
Joint report of the Town Clerk and Commissioner.

For Information
(Pages 13 - 18)

6. **NATIONAL LEAD FORCE PERFORMANCE REPORT**
Report of the Commissioner.

For Information
(Pages 19 - 38)

7. **NATIONAL LEAD FORCE (NLF) UPDATE**
Report of the Commissioner.

For Information
(Pages 39 - 44)

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

For Information
(Pages 45 - 48)

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

For Information
(Pages 49 - 62)

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

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

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

For Decision

Part 2 - Non-Public Agenda

13. **NON-PUBLIC MINUTES**
To agree the draft non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 3rd of October 2022.

For Decision
(Pages 63 - 66)

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

For Information
(Pages 67 - 68)

15. **COMMUNICATIONS & STRATEGIC ENGAGEMENT: QUARTERLY UPDATE**
Joint report of the Town Clerk and Commissioner.

For Information
(Pages 69 - 72)

16. **ECONOMIC CRIME LEVY BID**
Report of the Commissioner.

For Information
(Pages 73 - 76)

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

For Information
(Pages 77 - 90)

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

19. **ANY OTHER BUSINESS THAT THE CHAIR 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
Monday, 3 October 2022

Minutes of the meeting of the Economic and Cyber Crime Committee of the City of London Police Authority Board held at Committee Rooms, 2nd Floor, West Wing, Guildhall on Monday, 3 October 2022 at 3.00 pm

Present

Members:
Deputy James Thomson (Chair)
Alderman Professor Emma Edhem
Dawn Wright
Andrew Lentin (External Member)
Jason Groves
Alderman Bronek Masojada

Officers:

Richard Holt	-	Town Clerk's Department
Alix Newbold	-	Director, Police Authority
Oliver Bolton	-	Police Authority
Peter O'Doherty	-	Assistant Commissioner, City of London Police
Charlie Morrison	-	City of London Police
Hayley Williams	-	City of London Police
Andrew Gould	-	City of London Police
Melissa Panzi	-	Innovation and Growth Department
Lucy Cumming	-	City of London Police

1. **APOLOGIES**
Apologies were received from the Deputy Chair Tijs Broeke, James Tumbridge, Deputy Graham Packham, Deputy Graeme Doshi-Smith and the Chair of the Policy and Resources Committee Deputy Christopher Hayward.

2. **MEMBERS' DECLARATIONS UNDER THE CODE OF CONDUCT IN RESPECT OF ITEMS ON THE AGENDA**
The Chair Deputy James Thomson made a declaration as non-executive board member of Economic and Cyber Crime Academy and as a member of the Serious Fraud Office board.

3. **MINUTES**
The Committee considered the draft public minutes and non-public summary of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May.

RESOLVED- That the public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May be approved as an accurate record.

4. **PUBLIC OUTSTANDING REFERENCES**

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

Further to action 12/2021/P Officers provided an update on the engagement with FinTech firms, including the scheduled events over the next quarter. The Chair added that lots of good work in this area was being completed which was not all captured in the note provided to the Committee. It was noted that there was an event being planned to take place in January 2023.

Updating on the action 6/2022/P regarding the number of Action Fraud Call Handlers Officers confirmed that this number was now at its highest level and there was an expectation of an improvement in the service as a result.

Following an update on action 1/2022/P regarding the City of London Police involvement with insurance companies it was noted that a discussion with the new head of the Association of British Insurance would be undertaken with an update to the next 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 of the Executive Director Innovation and Growth on the Innovation and Growth Update of Cyber & Economic Crime related activities.

The Chair commented that further progress on this project should not be delayed in order to fit in with the City of London Corporation's governance processes and instructed Officers to take this forward as promptly as possible.

Replying to a Member's query the process for the development of technology adoption from the Cyber Innovation Challenge was outlined to the Committee.

RESOLVED- That the report be noted.

6. **NATIONAL LEAD FORCE PERFORMANCE REPORT Q1: APRIL – JUNE 2022**

The Committee received a report of the Commissioner on the National Lead Force Performance Report Q1 April- June 2022. The Committee received an accompanying presentation from Officers on the City of London Police's role as National Lead Force for fraud.

In response to a Member's query Officers confirmed that there was a dedicated team in place with responsibility for the recovery of assets.

Following a request from the Committee, Officers undertook to include a metric on the number of call handlers and response times to the Service's success measures.

A Member requested further information on the process for establishing future trends in fraud. Officers confirmed the extensive process for establishing these trends

including engagement with effected business and national bodies to develop a cross sector perspective.

Officers confirmed, in response to concerns expressed by the Committee, that a fully funded City of London Police communication team with responsibility for effective communication of matters relating to the fraud and cyber crime. In addition, the specific methodology for engagement with small and medium size businesses was explained.

RESOLVED- That the report be noted.

7. **NATIONAL LEAD FORCE UPDATE**

The Committee received a report of the Commissioner which provided the National Lead Force update.

Responding to a Member's query it was confirmed that an update on the work for cyber crimes which are not financial in nature would be provided in future reports.

Following discussion by the Committee Officers outlined the proactive and reactive policies for removing websites involved in the criminal activity including the use of artificial intelligence. The Chair noted that, in the long term, this action would likely be led by artificial intelligence systems.

The Committee discussed the possibility for tougher sentences for fraud related offences and requested that Officers explore opportunities for providing this feedback to the Government.

Replying to the Chair's comment the national work of the Economic and Cyber Crime Academy was explained to the Committee. In addition, it was confirmed that the Academy was in part, funded by POCA funds.

RESOLVED- That the report be noted.

8. **CYBER GRIFFIN UPDATE**

The Committee received a report of the Commissioner which provided an update on Cyber Griffin.

The Committee discussed how best to make the Cyber Griffin initiative nationally integrated and requested that Officers develop a strategic option on this for the Committee's consideration.

Responding to a Member's query the sector-by-sector engagement strategy was explained noting that continuous work was being undertaken to make this engagement more impactful and valuable.

RESOLVED- That the report be noted.

9. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
Following the Chair's question an update on Economic and Cyber Crime Member reference group was provided to the Committee. It was noted that, whilst the reference group was designed to facilitate wider Member engagement beyond the Committee, Committee Members should also be invited to the reference groups meeting.

10. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT**
There was no urgent business considered in the public session.

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

12. **NON-PUBLIC MINUTES**
The Committee considered the draft non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May.

RESOLVED- That the non-public minutes of the previous meeting of the Economic and Cyber Crime Committee held on the 13th of May be approved as an accurate record.

13. **NON-PUBLIC OUTSTANDING REFERENCES**
The Committee received a joint report of the Town Clerk and Commissioner on the non-public outstanding refences from the previous meeting.

RESOLVED- That the report be noted.

14. **STRATEGIC COMMUNICATIONS & ENGAGEMENT: QUARTERLY UPDATE- ECONOMIC AND CYBER CRIME**
The Committee received a report of the Commissioner on the Strategic Communications and Engagement Quarterly Update Economic and Cyber Crime.

RESOLVED- That the report be noted.

15. **NPCC CYBER CRIME PORTFOLIO- CYBER CRIME PLAN 2022-23**
The Committee received a report of the Commissioner on the NPCC Cyber Crime Portfolio Cyber Crime Plan 2022-23.

RESOLVED- That the report be noted.

16. **NPCC CYBER CRIME PORTFOLIO- CRYPTOCURRENCIES AND VIRTUAL ASSETS**
The Committee received a report of the Commissioner on the NPCC Cyber Crime Portfolio cryptocurrencies and virtual assets.

RESOLVED- That the report be noted.

17. **NPCC CYBER CRIME PROGRAMME - BENEFITS EVALUATION 2021-22**
The Committee received a report of the NPCC Cyber Crime Programme Benefits Evaluation 2021-22.

RESOLVED- That the report be noted.

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

The Committee agreed to suspend Standing Order 40 and extend the meeting beyond two hours.

RESOLVED- That the report be noted.

19. **QUESTIONS ON MATTERS RELATING TO THE WORK OF THE COMMITTEE**
There was one question received in the non-public session.

20. **ANY OTHER BUSINESS THAT THE CHAIRMAN CONSIDERS URGENT AND WHICH THE COMMITTEE AGREE SHOULD BE CONSIDERED WHILST THE PUBLIC ARE EXCLUDED**
There was no urgent business considered in the non-public session.

The meeting ended at 5:03pm

Chair

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

This page is intentionally left blank

12/2021/P	**4 November 2021** Innovation & Growth	By utilising the City and Mayoralty's convening power there would be better engagement with smaller FinTech firms. It was suggested that a FinTech specific event could be arranged.	Assistant Commissioner/ Exec Director for Innovation and Growth	**Complete**- AC O'Doherty updated at the October 3 ECCC to say that an event was being planned for January 2023.
7/2022/P	**3 October 2022 Item 5- Innovation & Growth – Update of Cyber & Economic Crime related activities**	Regarding the City of London Police scope for investigation types (Motor, travel, other) with insurance companies it was noted that a discussion with the new head of the Association of British Insurance would be undertaken with an update to the next meeting of the Committee.	Commissioner of Police	**Complete**- IFED currently has over 200 live investigations. These comprise frauds relating to vehicle insurance, holiday insurance claims, personal injury/public liability (such as tripping over and obstacle in a restaurant), pet insurance, home and contents and life assurance. The majority of referrals relate to vehicle insurance. Fraud in this area is prevalent as, for example, low paid people who may not own a home or go on holiday often seek cheap insurance to allow them to undertake work which requires access to a vehicle making them vulnerable to 'Ghost Broking'. In addition the investigations of some vehicle fraud types presents a high level of public interest. For example induced accidents and 'slam ons' can result in injury to third parties, a risk not present in other fraud types **Product Line** | **Volume**

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>
<table>
<tr><td>Motor Insurance</td><td>119</td></tr>
<tr><td>Property Insurance</td><td>41</td></tr>
<tr><td>Travel Insurance</td><td>14</td></tr>
<tr><td>Life & Medical Insurance</td><td>8</td></tr>
<tr><td>Public Liability</td><td>7</td></tr>
<tr><td>Personal Insurance</td><td>4</td></tr>
<tr><td>Pet Insurance</td><td>2</td></tr>
<tr><td>Other Insurance Types</td><td>11</td></tr>
<tr><td>Total</td><td>206</td></tr>
</table>
</td>
</tr>
<tr>
<td>8/2022/P</td>
<td>3 October 2022 Item 6-

National Lead Force Performance Report Q1: April – June 2022</td>
<td>Following a request from the Committee Officers undertook to include a metrics on the number of call handlers and response times to the service’s success measures.</td>
<td>Commissioner of Police</td>
<td>Complete-Average speed of answer and call abandonment rates data has been included under measure 1A in the Q2 NLF Performance Update report on the agenda.</td>
</tr>
<tr>
<td>9/2022/P</td>
<td>3 October 2022 Item 8- Cyber Griffin Update</td>
<td>The Committee discussed how best to make the Cyber Griffin initiative national integrated and requested that Officers bring an options paper back to the ECCC for the Committee’s consideration.</td>
<td>Commissioner of Police</td>
<td>In Progress- Active engagement with relevant Cyber Griffin stakeholders is taking place and work is being scoped. An update on this will be brough to the February ECCC.</td>
</tr>
</table>

Committee(s): Economic & Cyber Crime Committee	**Dated:** 25 November 2022
Subject: Communications & Strategic Engagement: Quarterly Update	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1
Does this proposal require extra revenue and/or capital spending?	**N/A**
If so, how much?	**N/A**
What is the source of Funding?	**N/A**
Has this Funding Source been agreed with the Chamberlain's Department?	**N/A**
Joint report of: Commissioner of Police & Town Clerk & Chief Executive PoI 106-22	**For Information**
Report authors: Lucy Cumming (Economic Crime Directorate, CoLP) & Ollie Bolton (Police Authority Team, CoLC)	

Summary

This report sets out a summary of key strategic meetings and events that have taken place between September and November 2022 which support the Policing Plan's operational priority of protecting the UK from the threat of economic and cyber-crime.

This update report follows the Stakeholder Engagement Plan approved by this committee at its last meeting, which aims to achieve the following:

a. Recognition of the value of City of London Police's role as the national policing lead for economic and cyber crime
b. Improved confidence in the national fraud and cyber reporting service and understanding of the roles of Action Fraud, policing and other organisations in improving outcomes for victims
c. Prevention of economic and cyber-crime through legislative and regulatory reforms and security measures undertaken by industry and the public
d. Improved policing capacity and capability to tackle economic and cyber-crime.

Recommendation

Members are asked to:

- Note the report.

Main Report

Background

2. Following the launch of the City of London Policing Plan 2022-2025, the Police Authority Board requested a communications and engagement plan to underpin the operational priorities. Alongside this, a commitment was made to the Economic & Cyber Crime Committee for a stakeholder plan for that particular area.

3. Members of the Economic & Cyber Crime Committee approved this communications and engagement plan at its last meeting on 13 May 2022. As a reminder, the strategic outcomes of this engagement plan are to achieve the following:

    a. Recognition of the value of City of London Police's role as the national policing lead for economic and cyber crime
    b. Improved confidence in the national fraud and cyber reporting service and understanding of the roles of Action Fraud, policing and other organisations in improving outcomes for victims
    c. Prevention of economic and cyber-crime through legislative and regulatory reforms and security measures undertaken by industry and the public
    d. Improved policing capacity and capability to tackle economic and cyber-crime.

Current Position

4. Listed below are the key strategic meetings and events which have helped to contribute towards the strategic outcomes listed above. These events are highlighted in the table below with a short summary of key thematic outcomes.

Engagement, Date	Which strategic outcome (see para 2) did this engagement link to?	Key outcomes
National Cyber Awards 26 September	A	Chief Officers in attendance.
International Cyber Expo 28 September	A, B	AC O'Doherty spoke at the event – promotion of CoLP
Director Homeland Security visit. 3 October	A,C	Visit with the Commissioner to discuss joint working
TISA Financial Fraud Conference (The Investing and Saving Alliance)	A	Commissioner attended.
Strategic Command Course, 5 October	A,D	AC O'Doherty lectured on course-vital to improve knowledge across Chief Officers nationally.
Interpol Liaison trip to Lyon	A	AC O'Doherty visit to Interpol to improve joint working.
SOCEX 10 October	A,B	AC O'Doherty spoke with the NECC. Promotion of CoLP and Fraud and Cyber Portfolio.
Economic Crime Briefing (Aviva) 11 October	A,B	National briefing, excellent attendance and Security Minister briefed.
Launch of the London Cyber Resilience Centre 25 October	A	Promotion of CRC initiative in London.
Cadets Passing Out Parade 25 October		
Cyber Resilience Centre Network Summit, 10 October	A	National event promoting Cyber Resilience Centre excellence.
APCC NPCC Conference 10 November	A, C	Promotion of CoLP to APCC and NPCC
Tackling Economic Crime Awards 14 November	A	Commander Nik Adams in attendance, recognising excellent working in this area. Awards went to PIPCU, CoLP and Lifetime Achievement to ex CoLP staff

5. In addition to the above, the Authority has continued to regularly engage with the Association of Police and Crime Commissioners (APCC) to support their Economic and Cyber Crime Portfolio (of which the PAB Chair is a deputy lead), identifying opportunities to amplify national campaign messaging (such as cyber awareness month and the recent investment fraud campaign. This allows Offices of Police and Crime Commissioners to increase the reach of key campaigns and strengthen their buy-in to the wider approach to tackling fraud and cyber-crime. This in turn

supports the Authority's aim of getting fraud and cyber-crime as a more visible priority in local police and crime plans.

6. Building on this further, the Authority has offered to host the next General Meeting of the APCC in January 2023, with the aim of having a significant proportion of the event dedicated to the fraud and cyber agenda. This will provide an opportunity to update PCCs on the developments nationally (with regional uplifts in investigators; progress with the procurement of the next generation fraud and cyber-crime reporting and analysis service; improvements to the current Action Fraud service; and developments in national policy) and also provide a platform for PCCs to showcase their efforts and a forum for discussion to overcome challenges that they may be facing.

7. Members of the Force and the Police Authority also attended a roundtable discussion on fraud on 19th October, organised by the Mayor's Office for Policing and Crime. This focused on improving the response to fraud across London and was well-attended by key stakeholders from across the system. Both the Force and the Authority look forward to seeing where this work may lead.

8. Engagement with Home Office officials continues to identify opportunities for ministerial visits and representation at key events in the City's calendar, with the aim of strengthen our links with Government on fraud and cyber-crime as it rises up the political agenda.

Corporate & Strategic Implications

9. Strategic implications – The City of London Policing Plan aligns with the City Corporation's Corporate Plan objectives 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 12. The development of this strategic stakeholder plans underpinning the objectives of the Policing Plan allows for better strategic and coordinated engagement with key stakeholders by the Force and plugs into the work being undertaken by the City of London Corporation.

10. Financial implications – None.

11. Resource implications – This work has shown that there are resource gaps within the Force to be able to fully manage the stakeholder engagement work.

12. Legal implications – None.

13. Risk implications – Implementing this strategic stakeholder engagement plan helps to mitigate against the Corporate Force Risk of "Loss of public confidence in professionalism and trust with Force".

14. Equalities implications – This report complies with the Public Sector Equality Duty 2010 and has no negative impact on people protected by existing equality legislation. Arguably, stakeholder work with communities should allow for a positive impact on people protected by the Equality Act.

15. Climate implications – None.

16. Security implications – None.

Conclusion

17. This report sets out the key highlights of the communications and engagement to support the Policing Plan operational priority of protecting the UK from the threat of economic and cyber-crime. It also sets out a list of upcoming and planned events over the next quarter for Members to note.

Appendices

- None

Background Papers

- Stakeholder Engagement Plan – Economic & Cyber Crime Committee (for decision) – 13 May 2022

Positive Media Coverage

- A new 'ghost broking' awareness campaign, launched by IFED and its partners, received coverage from Mail Online and regional publications. DCI Tom Hill was quoted.
- The i and Express shared a recent Action Fraud alert that warned consumers to watch out for fake text messages about the government's Energy Bill Support Scheme. An earlier alert, which stated that over 1,500 reports had been made about scam emails purporting to be from Ofgem, received further coverage in Sky News and the Express.
- Following a press announcement issued by CoLP, Insurance Times and Claims Mag reported that IFED arrested seven people during its intensification activity against travel insurance fraud. DCI Tom Hill was quoted.
- Mail Online published a statement from DCI Hayley King on fake emails purporting to be from Ofgem in an article that explored scams during the cost-of-living crisis. Information issued by Action Fraud about the fake Ofgem emails was also quoted by Metro.
- A hacker who made over £130,000 by selling unreleased music was jailed for 18 months following an investigation by PIPCU. The sentencing received widespread coverage, including BBC News, Sky News, ITV, Telegraph, Independent, Daily Mail, Evening Standard and Metro. DC Daryl Fryatt was quoted.
- ITV, The Mirror and Wales Online quoted DC Lloyd Haywood, after an IFED investigation saw a man sentenced in relation to a £50,000 'crash for cash' plot.
- James Thomson, Chair of the CoLP Authority Board, was quoted in City AM, Police Professional and Professional Security as they announced the launch of the Cyber Resilience Centre to protect businesses against cyber threats.
- Officers from PIPCU, assisted by colleagues from Support Group, seized £200 million worth of counterfeit designer goods during a raid in London. A press

announcement, featuring a quote from DCI Gary Robinson, was published by ITV News, the Express and MyLondon.

- ITV News, MailOnline, Yahoo! News and others quoted PIPCU's DC Daniel Dankoff after a man who threatened to publish a broadcasting company's customer records unless he was paid a ransom was jailed for 28 months.
- IFED's DCI Tom Hill was featured on ITV Evening News to help raise awareness of ghost broking and how the public can protect themselves against it.
- A press announcement issued by CoLP after four men were sentenced for running an investment scam that conned more than 340 people out of £5.4 million received coverage in the Evening Standard, Yahoo! Finance and International Adviser.
- MyLondon and FinExtra quoted the DCPCU's DC Dan Jordan after a man was jailed for two-and-a-half years for a £280,000 courier fraud scam.
- Further coverage of a PIPCU raid, in which £200 million worth of counterfeit designer goods were seized in west London, appeared in the Metro (print) and Securing Industry.

Lucy Cumming
Head of Economic Crime Strategy and Government Affairs
E: lucy.cumming@cityoflondon.police.uk

CITY OF LONDON POLICE
National Policing Lead For Fraud

National Lead Force Performance Report

Q2: July – September 2022

Performance Assessment

The dashboard provides an assessment of City of London Police (CoLP) performance against the National Lead Force (NLF) aims and objectives as set out in the National Lead Force Plan 2020-2023 (NLF Plan). The NLF Plan was approved by the City of London Police Authority in October 2020. The plan sets out how CoLP will improve the national response to fraud. It reflects NLF's contribution and commitment to the National Fraud Policing Strategy and the National Economic Crime Centre's (NECC) five-year strategy. The NECC leads the 'whole system' to drive down the growth in fraud on behalf of the UK Government.

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

			Q1	Q2
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.	GOOD	GOOD
Outcome 2	**Disrupt fraudsters**	We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.	ADEQUATE	GOOD
Outcome 3	**Investigate and prosecute**	We successfully lead the local to national policing response in investigating and prosecuting fraudsters, ensuring better outcomes for victims.	GOOD	GOOD
Outcome 4	**Raise awareness and prevent crime**	We raise awareness of the threat and prevent fraud impacting people and businesses.	ADEQUATE	GOOD
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.	ADEQUATE	GOOD

CITY OF LONDON POLICE

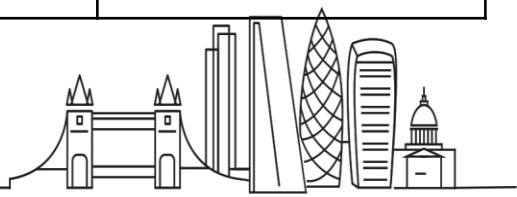
The grading criteria can be found in Appendix A – Performance Assessment Criteria

Executive Summary

Outcome 1 GOOD	Outcome 2 GOOD	Outcome 3 ADEQUATE	Outcome 4 GOOD	Outcome 5 GOOD
Supporting and safeguarding victims	**Disrupt fraudsters**	**Investigate and prosecute**	**Raise awareness and prevent crime**	**Building capabilities**
Action Fraud victim satisfaction is above the benchmark on both channels, an improvement from Q1. NECVCU engagement was up by 54%. Vulnerable victims made up 13% of level 2 cases, down from the previous quarter. Repeat victims stay under 1% of total contacts. 100% of victims identified as vulnerable were sent for safeguarding within 7 days. Sending fulfilment letters and Protect emails met the timeliness targets. NFIB Cyber have met their review and dissemination targets, with 100% of cybercrime reports disseminated. The project to alert banks to accounts used in fraud suffered technical issues, and numbers are down on 21/22.	14 disruptions were claimed against NLF OCGSs, less than the quarterly average from the previous year. Of these, 1 was classified as a Major disruption. NLF carried out a total of 11 POCA activities, above the 21/22 quarterly average of 8 and the 21/22 Q2 total of 7. During Q2, almost double the Q1 total of disruptions were recorded. Disruption activity focused on websites, and in September 3,896 .com domains were suspended, with over 210 affected brands being identified. Disruptions to other technological enablers also rose throughout the quarter.	The number of judicial outcomes recorded nationally is 17% below the 21/22 quarterly average, and CoLP Q2 judicial outcomes are 90% lower. 100% of Home Office forces remained in the compliant category for reporting outcomes. LFOR engaged in preparing for a number of national and multi-agency campaigns which will take place in Q3. These include an intensification focusing on investment fraud, and working with the MPS Cyber Crime unit to target the owners and users of a criminal website.	The number of social media posts increased compared to Q1. Despite external posts being paused for Op London Bridge, #ReportThePhish and #SunSeaAndScam received media notice and high impressions throughout the summer. A lower number of campaigns were run, due to the school holiday period, as teams focused on planning for the autumn months. These campaigns included an intensification period by PIPCU, and a number of effective social media campaigns.	The number of delegates trained by the Economic and Cybercrime Academy rose by 14% from Q1 to Q2. Satisfaction levels fell slightly from 91% to 86%. NLF teams work closely with a wide range of law enforcement and government agencies, banks, and industry partners. New initiatives this quarter include a national fraud campaign, and an international fraud collaboration with Interpol. Establishment of a new Fraud Policing Network continues. By the end of 2022-23 the target is for the network to have 122 staff, at the end of Q2, 57 posts are in place (47%).

CITY OF LONDON POLICE

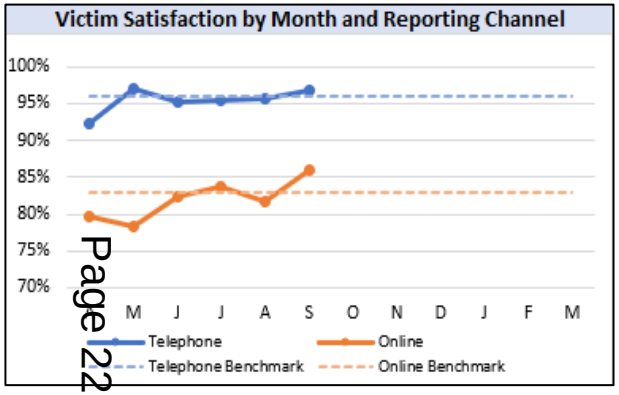
The grading criteria can be found in Appendix A – Performance Assessment Criteria

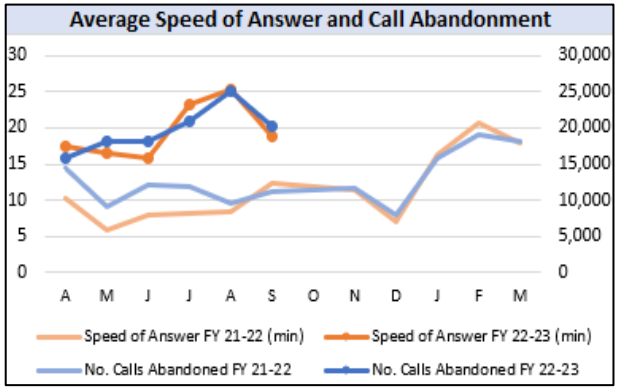


Outcome 1: *Supporting and Safeguarding Victims.*

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





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 Q2 opted to provide satisfaction feedback to the confirmation fulfilment survey. Over 1.56M confirmation survey links have been delivered to date, with 17,444 respondents (1.1%) opting to provide satisfaction feedback, including free text responses which are used to continuously improve the service.

1.A. – The Action Fraud survey indicates that satisfaction with the telephone reporting service in Q2 remained stable and within target at 96%. This is in line with Q2 of FY 21/22 which also saw a satisfaction rate of 96%. Overall satisfaction levels in this area remain high over the long term, and negative feedback received in Q2 is largely attributable to frustration regarding increased call waiting times. Measures are now in place to address this, with September seeing a significant reduction of over 6 minutes from the 25.35 high in August to 18.72 minutes, due to increased staffing numbers.

The technology issues which impacted the distribution of fulfilment letters (which contain the survey) in the previous quarter have now been resolved and response levels have returned to anticipated volumes.

1.B. – Online satisfaction saw improvement in Q2, coming in just above the benchmark at 84% across the quarter, and with September noting a high of 86%. September saw the highest response rate, and the higher the response rate, the more confidence there is that the results are representative of those using the service.

CITY OF LONDON POLICE

The Action Fraud surveys are in response to victim's first contact with NLF when reporting a fraud, and are not representative of the end to end victim journey.

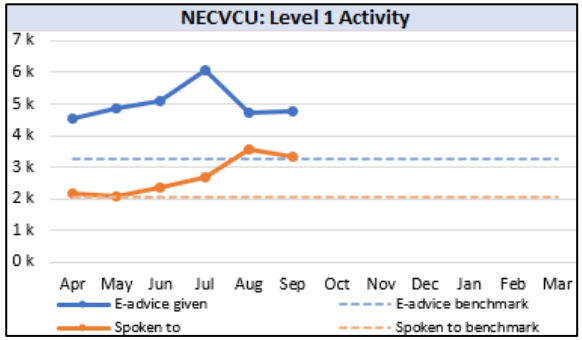
Outcome 1: *Supporting and Safeguarding Victims.*

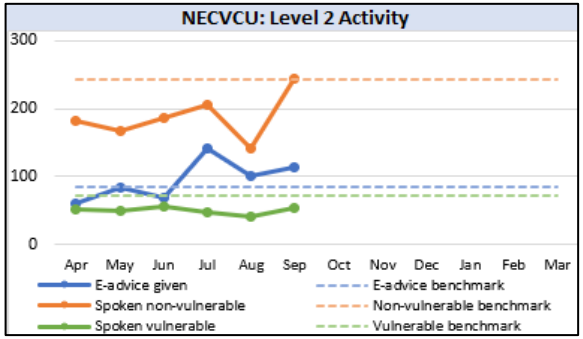
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

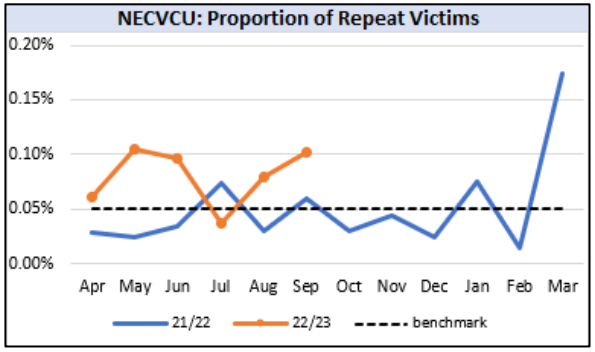
Success Measures:	
C. To maintain the level of repeat victimisation after NECVCU contact to under 1%.	GOOD
D. To increase the proportion of vulnerable victims receiving Level 2 support.	ADEQUATE
E. To increase the number of victims contacted by NECVCU.	GOOD

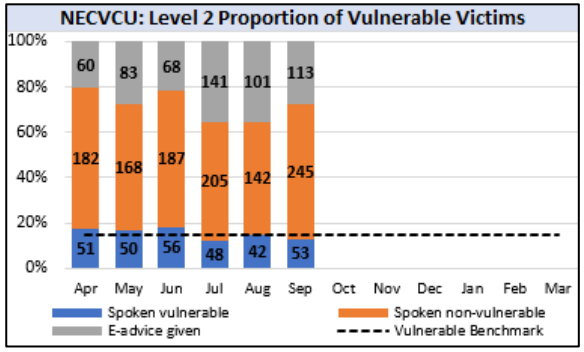
The National Economic Crime Victim Care Unit (NECVCU) supports forces at a local level, delivering care to victims of fraud and cyber-crime, allowing for a consistent and national standard of care and support. The **Level 1** service gives Protect/Prevent advice to non-vulnerable victims of fraud. The **Level 2** service engages with victims when vulnerability is identified, and by giving crime prevention advice and signposting to local support services helps the victim to cope and recover from the fraud.

1.C. – In Q2 there were 22 victims identified as repeat victims, up from the 2021/22 quarterly average of 9, but below the 1% target at 0.07% of victims engaged with during the period.
1.D. – The number of vulnerable victims spoken to by the Level 2 service was slightly less than in Q1 (143 down from 157). Proportionally, vulnerable victims made up 13% of Level 2 cases as the team contacted a higher number of non-vulnerable individuals.
1.E. – When compared against the 2021/22 Q2 total (20,231) and the 21/22 quarterly average (19,931), victim engagement was up by 52% and 54% respectively, with 30,667 contacts across both levels. This is in line with the increase in the number of forces covered by the Level 1 service, from 20 in 21/22 to 37.





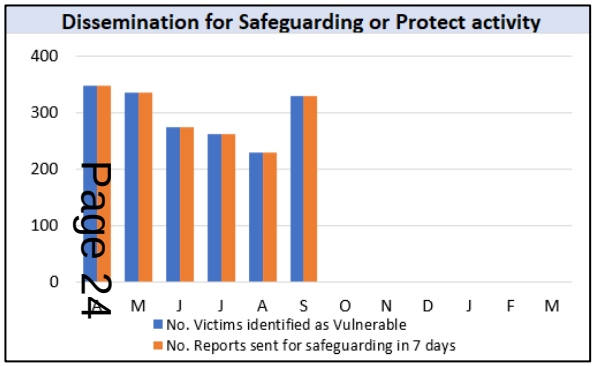


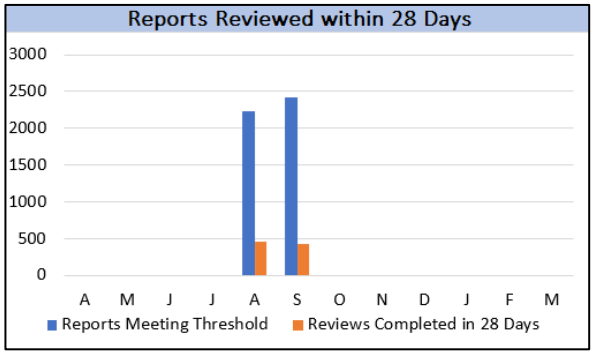


Outcome 1: *Supporting and Safeguarding Victims.*

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

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





1.F. – To identify potentially vulnerable victims, a search is run on all reports of fraud, looking at agreed 'risky words' which highlight a vulnerability risk for the victim - for example suicide, mental health, threats to life or violence.

In Q2, 821 reports were confirmed as coming from vulnerable victims, and 100% were sent to forces for victim support within 7 days of the report being downloaded to the system.

1.G. – The process for gathering this data is under development and partial data is only available from August 2022. The number of reviews recorded relates to non-complex crime and thus reflects the work of two of the three NFIB review teams.

There are technical limitations for crimes with multiple report cases, meaning workarounds are in place. The recording of these makes it difficult to identify the timeframes involved, and a solution is being developed which will give a fuller picture of the threshold and review process.

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

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

1.I. – The NFIB have a number of advice letters, tailored to each fraud type, which are emailed to victims on a weekly basis. This service is known as 'Send in Blue'. In August 2021 this process was automated, and the success rate went from a low of 59% in June, to an average of 99.69% for the rest of 2021/22. In Q2 22/23, the success rate of Send in Blue was 99.9%.

Outcome 1: *Supporting and Safeguarding Victims.*

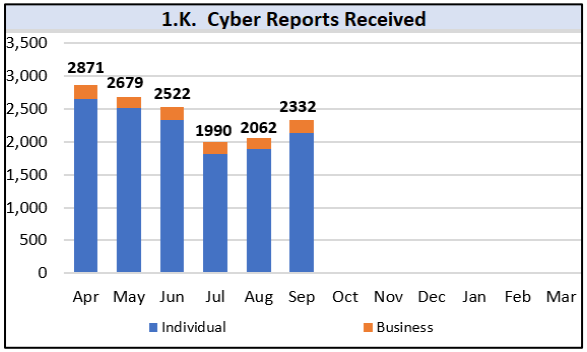
NLF Role: We provide a service for victims that is accessible, user-friendly and easy to engage with, and we successfully support and safeguard victims.

Success Measures:	
J. To review all unclassified cyber related Action Fraud reports to determine their viability for dissemination, within 7 days.	OUTSTANDING
K. To review and disseminate all Action Fraud reports classified with an NFIB Cybercrime code, within 7 days.	ADEQUATE
L. To respond to all live cybercrime reports, within 2 hours of reporting.	GOOD
M. To determine and respond to all reports of cyber dependent crime identified as having a victim vulnerability factor, and disseminate for safeguarding activity, within 72 hours of reporting.	ADEQUATE
N. All businesses reporting cyber enabled crime to receive Protect advice within 72 hours of reporting.	GOOD

1.J. – NFIB Cyber review all unclassified cyber related Action Fraud reports within 7 days as a standard process. In the last quarter this has been reduced to 72 hours. This is a qualitative update and quantitative data is being sought.

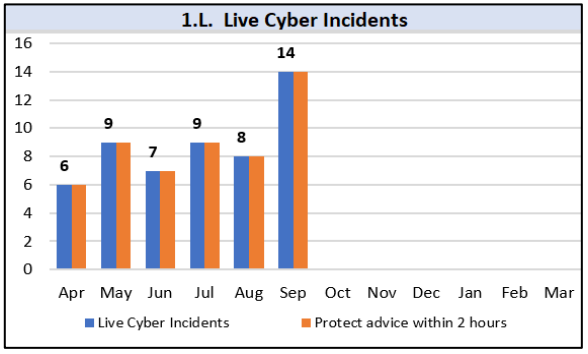
1.K. In Q2, 6,384 reports were classified with a Cybercrime code. Of these, 100% were disseminated for Protect or Pursue. This measure is being reviewed and a process for reporting timeliness will be explored for Q3.

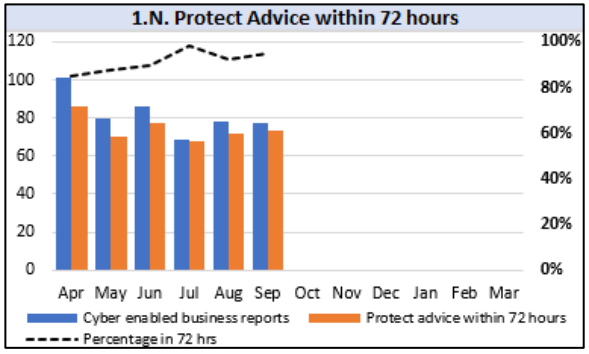
1.L. – 31 live cyber incidents were recorded in Q2, and each one was reviewed and a response sent within 2 hours.



1.M. – The Cyber Review team are piloting a process to identify vulnerability within cyber crime reports, to ensure support is provided to the victim as soon as possible. The team complete this daily, and where vulnerability is identified safeguarding requests are disseminated the same day.

1.N. – 95% of businesses reporting cyber enabled crime were provided Protect advice within 72hrs. As the processes have become embedded this has improved consistently.

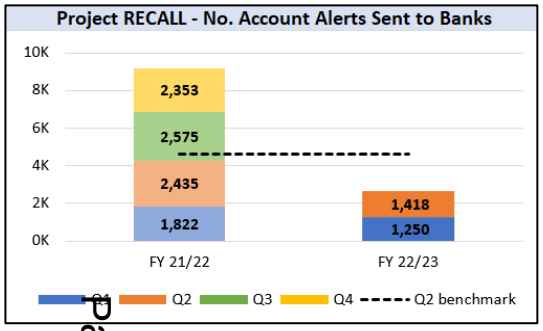


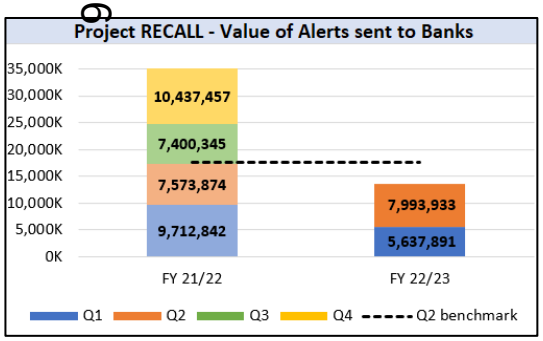


Outcome 1: *Supporting and Safeguarding Victims.*

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

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





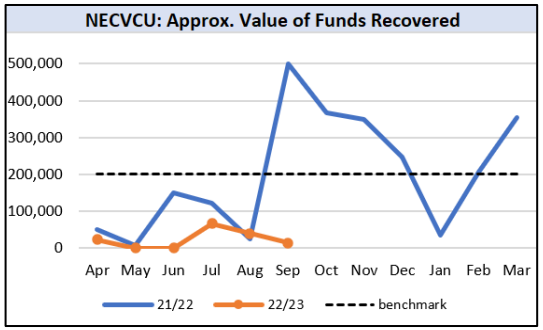
Project RECALL is an initiative to alert banks to accounts used in fraud. Although automation allows more reports to be sent out, there have been numerous technical issues with the system in the last two quarters. These issues are resolved as quickly as possible, however due to the short window for potential alerts to be released, this impacts the overall volume of alerts. Work is ongoing to improve the reliability of this service. Additionally, overall fraud reporting is down by over 22.5% in the last 12 months compared to the previous year, which has reduced opportunities for alerts to be sent out.

In Q2 CoLP alerted banks to 1,418 accounts used to receive the proceeds of fraud, the value of which was £7,993,933. The system for banks to confirm the value of repatriated funds is not automated, and the banks are proactively asked for feedback. In Q2 £27,148 was confirmed to the NFIB, but as not all banks responded there are likely to be significantly higher volumes of funds being safeguarded for victims.

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.

The number of **NECVCU** victims with confirmed recoveries, and the associated value of those recoveries is dependent on the victim informing the NECVCU. Since January 2021 NECVCU have supported 86 victims to recover £2,409,301.56.

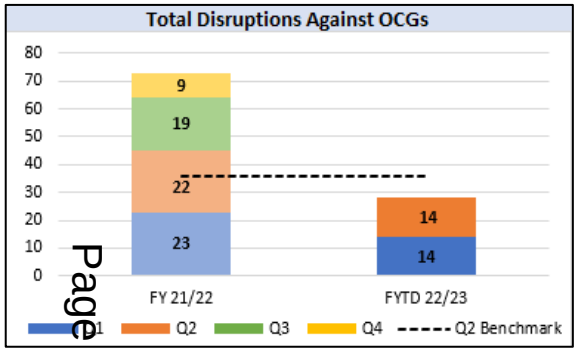
They have also provided additional support to 152 service re-users since August 2018 preventing a possible £2,447,808 being lost to economic crime.

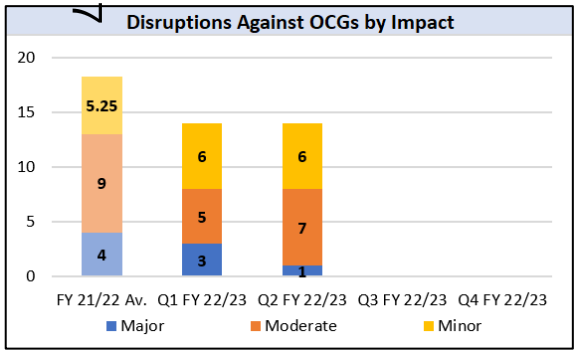


Outcome 2: *Disrupt Fraudsters.*

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

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





There are currently 67 mapped Organised Crime Groups (OCGs) under investigation by National Lead Force teams, up 42% from the 21/22 average of 47. Five new OCGs were mapped in the quarter, and one was closed.

There were 14 disruptions claimed against NLF OCGSs in Q2, which is less than the quarterly average of 18 from the previous year. Of these, 1 was classified as a Major disruption. There were also 7 Moderate and 6 Minor disruptions recorded.

There is currently only 1 Economic Crime OCG group that falls within the highest quartile of harm scoring OCGS and no disruptions were made against it in Q2.

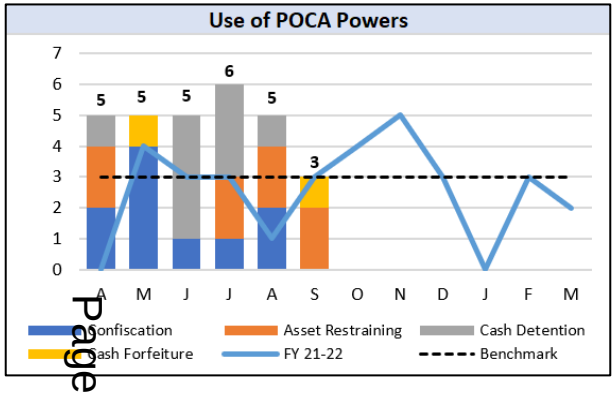
Please note, all DCPCU Disruptions have now been represented within these figures, including those assigned to the Metropolitan Police. This gives a more balanced picture of DCPCU disruption activities.

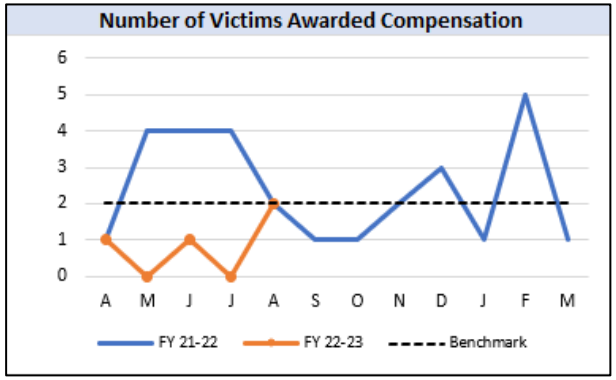
- A major disruption represents the OCG being fully dismantled or impacted at a key player level. In this instance, a key nominal pleaded guilty and was sentenced to 22 months suspended for 2 years, effectively shutting down the OCG.
- Major disruptions are not claimed until after court hearings and moderation panels, meaning there are a number of major disruptions yet to be claimed due to court backlogs.
- The 7 Moderate and 6 Minor disruptions relate to arrests of nominals and seizure of monies.

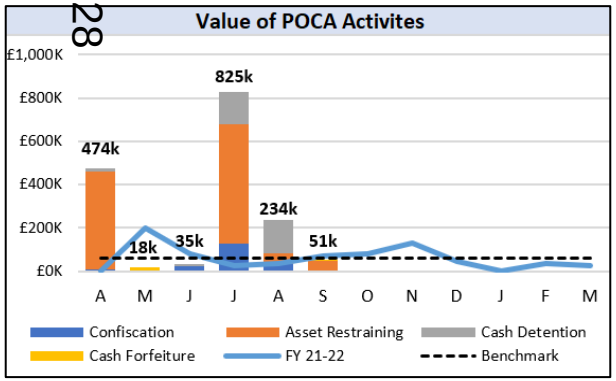
Outcome 2: *Disrupt Fraudsters.*

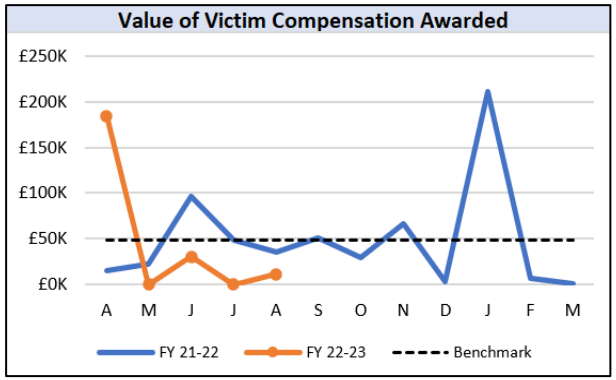
NLF Role: We disrupt fraudsters that operate domestically and from overseas in order to make it harder for them to commit crime here in the UK.

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









In Q2, Operational Fraud teams and Funded Units carried out a total of 11 POCA activities. This is above the 21/22 quarterly average of 8 and the 21/22 Q2 total of 7.

Most of the activity focused on asset restraints (4) and cash detentions (4). The greatest value came from the two asset restraining orders carried out in July and August which totalled £600,000.

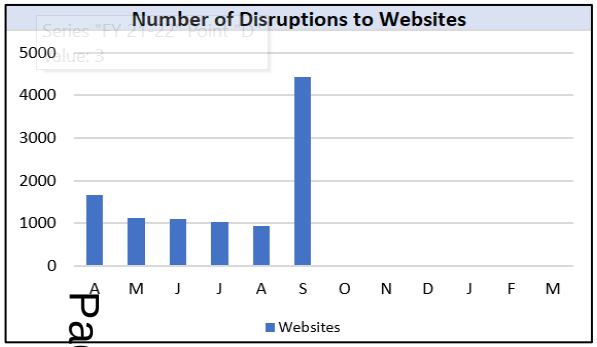
Although below the 21/22 benchmark, teams worked to ensure that 2 victims were awarded a total of £11,284 compensation by the Courts.

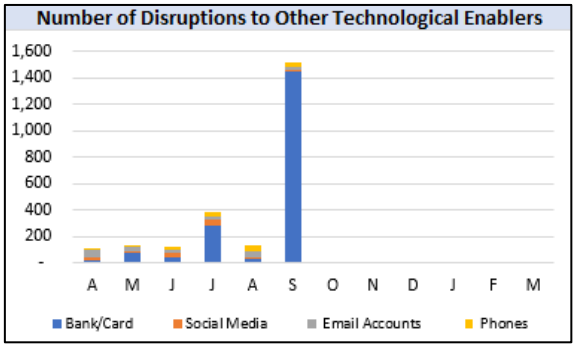
In July, PIPCU carried out a week of intensification at Cheetham Hill where a number of warrants were executed. 9 people were arrested and seizure of hundred of tonnes of counterfeit goods were taken from commercial properties. Counterfeit prescription drugs and thousands of pounds of cash were also seized.

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	OUTSTANDING





During Q2, a total of 8,399 disruptions were recorded, almost double the Q1 total of 4,299. Disruption activity across departments focused on websites, as PIPCU's operation to suspend websites selling counterfeit items went international following a decrease in the number of .uk domain sites being registered. Partnerships with various registrars have increased and in September due to this new approach, 3,896 .com domains were suspended, with over 210 brands being identified as affected companies.

Disruptions to other technological enablers rose throughout the quarter, reaching a peak in September, when DCPCU disrupted 1,451 bank accounts, with a value of £1,018,206. This was due to an intelligence led investigation where the principal subject had been identified making significant payments to 'carding sites' - illicit marketplaces used to trade compromised accounts. The subject's devices were seized and a significant number of compromised accounts were identified and protected before they could be subjected to loss.

City of London Police and National Cyber Security Centre Suspicious Email Reporting and Takedowns: NCSC & COLP receive reporting of suspicious emails from the public via SERS, which launched 21 Apr 2020. As of 30th September 2022, the number of reports received stand at more than 14,400,000 with the removal of more than 100,000 scams across 184,000 URLs. The public are sent large volumes of scam messages every day, many of which will be blocked by spam filters or otherwise ignored.

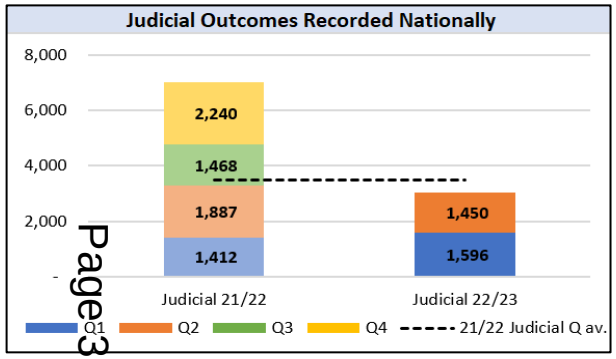
In Q2 there were more than 21,000 suspicious emails reported per day to NCSC and COLP, in addition to around 565 cyber-enabled crimes reported by victims to Action Fraud. From these suspicious emails, we identified over 460 new pieces of infrastructure (websites, servers, or emails) per day, i.e., about 2.2% of scam messages the public sent us contained unique knowledge of something malicious.

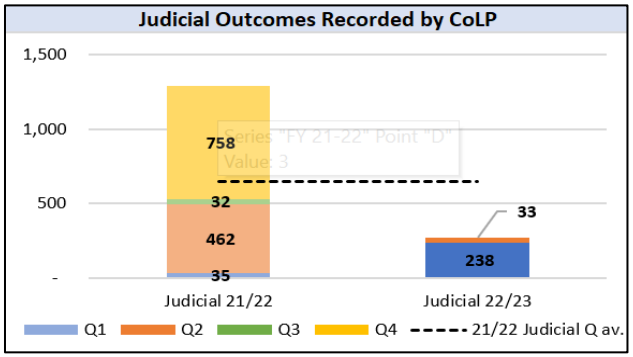
Calculating the value of 'actual loss' and 'potential loss saved' is complex and teams do not currently use the same methods. It is our aim to capture the impact of disruptions on victims and options are being explored to bring these in line.

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





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

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

FY 22/23 FYTD	No. Forces
Compliant (4-6 Returns)	45
Partially Compliant (n/a)	0
Non Compliant (0-2 Returns)	0

Forces are required to provide outcome information to CoLP every month, matched against their NFIB disseminations. In Q2, all forces provided their return each month. The National Coordinators will continue to engage with forces to ensure this 100% compliance can be maintained throughout the year.

At the end of Q2, the national judicial outcome rates (England and Wales) are 8.0% for 2019/20, 5.7% for 2020/21 and 4.8% for 2021/22. There are still outstanding disseminations for each year either being investigated or awaiting closure - which means the outcome rate is likely to increase over time and these figures are subject to change.

The COLP judicial outcome rate is 23% for 2019/20, 10% for 2020/21 and 38% for 2021/22, far higher than the national averages. The COLP NFA rate is currently 6% for 2021/22, which is below the national average of 47%.

COLP has now recorded 271 Judicial outcomes for the 6 months to 30th September 2022/23, but this is below the comparative period for 2021/22 where 497 were recorded. Sept 2021 saw 400 plus driven by 3 large operations.

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.	GOOD

National Operational Activity

During this period LFOR have been engaged in preparing for **Operation Broadway, an intensification focusing on investment fraud.** This will include working with the NECC and trading standards to coordinate a Pursue and media campaign nationally**.** The intensification will run for two weeks from the week commencing 17th October.

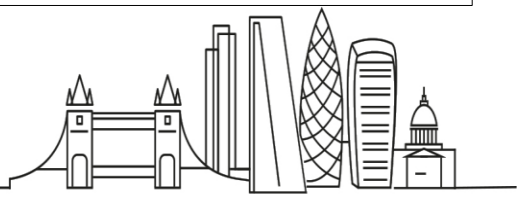
Preparation is taking place for **Operation Elaborate,** working with the MPS Cyber Crime Unit to target the owners and users of a criminal website. LFOR are coordinating the allocation of evidence packs out to ROCUs and forces targeting suspects throughout the UK. Following executive action planned for November, LFOR will coordinate the collection of results.

During this quarter the LFOR team has seen a number of staff abstractions caused by local and national events requiring a large policing response.

National and International Coordination and Assistance

- LFOR assisted other Forces and Regions with **16 requests for assistance** during Q2 2022-23. The requests were for arrests, warrants to be executed, supporting premises searches, and the gathering of evidence. This is a key role of LFOR who will provide Operational and Investigative support to all UK Forces and Regions to progress cases with enquiries in London. A high number of OCG activity that impacts victims across the country have links to London, and by providing such support LFOR are supporting partners in expediting positive outcomes and disruption opportunities.
- As the **National lead for Courier Fraud**, LFOR continue to support the Intelligence Development Team with analysis and dissemination of data to support PURSUE activity across the UK. Courier fraud offences have reduced by 60% compared to this time last year. During this quarter Crime Stoppers have been running a courier fraud campaign, which will change to a Romance Fraud campaign in the next quarter.
- LFOR received and developed 5 cases that were subject of **Case Acceptance Plans** for consideration by NLF Operations. This compares to 8 cases the previous quarter.
- There have also been 83 **International requests for assistance** from Foreign Law Enforcement Agencies. These are managed within LFOR, and during this quarter the highest number of requests were from Germany. The overall number of International requests was 49 for the previous quarter.

CITY OF LONDON POLICE
Lead Force Operations Room



Outcome 4: *Raise Awareness and Prevent Crime.*

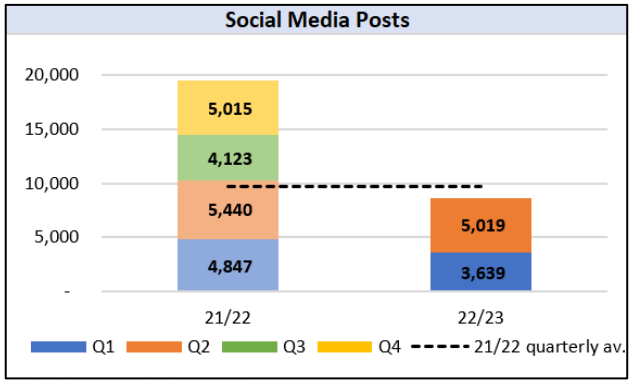
NLF Role: We raise awareness of the threat and prevent fraud impacting people and businesses.

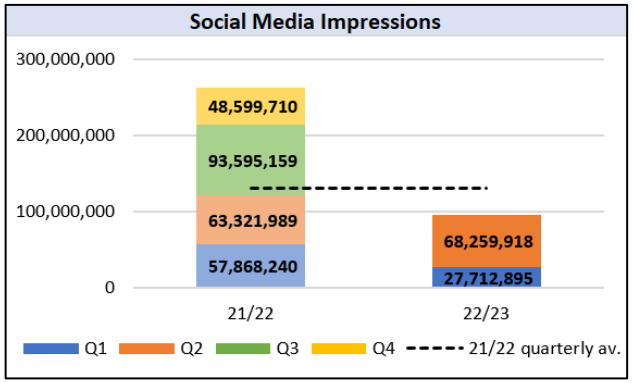
Success Measures:	
A. To increase the number of Social Media posts.	ADEQUATE
B. To increase the reach of Social Media posts (impressions).	GOOD

Across the various teams engaging on social media, improvement was made in the number of posts and impressions received. The number of posts were in line with the 21/22 Q2 and quarterly average. Engagement was higher, driven in particular by the NFIB Cyber Protect team who saw 35,000,000 impressions in July alone.

Notable campaigns included Cyber Protect's #ReportThePhish, and Action Fraud posted a number of alerts about fake Royal Mail emails and launched their new BSL service. IFED's #SunSeaAndScam travel insurance ran through the summer holiday period. The Fraud and Funded units posted about their significant arrests and campaigns, and PIPCT launched a LinkedIn page, expanding their online presence.

Across the quarter, the Media Team oversaw 9 press releases and 3 interviews, including newspaper and television interviews which resulted in positive news coverage. The NFIB also released 4 alerts through its digital community messaging platforms, which has been upgraded and can now reach approximately 500,000 users each time an alert is sent. All external comms were paused from 8-19 September, due to Op London Bridge. From 20 September, we followed the government guidance that police forces should return to social media gradually.





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

Impressions are defined as the number of people your content is visible to, while reach refers to the number of people engaging with your content through likes, comments and shares.

Outcome 4: *Raise Awareness and Prevent Crime.*

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

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

Police Intellectual Property Crime Unit

In July, PIPCU delivered the first of its quarterly intensification campaigns targeting the Cheetham Hill area of Manchester (synonymous with counterfeit goods).

This was a multi-agency campaign led by PIPCU to:

- Pursue and disrupt OCGs,
- Prevent criminal activity by the serving of Cease and Desist notices to deter people from committing or continuing to engage in crime,
- Protect by the use of increased media messaging to educate the public around the harm caused by counterfeit goods.

9 people were arrested and hundreds of tonnes of counterfeit goods were taken from commercial properties. Counterfeit prescription drugs and thousands of pounds of cash were also seized.

Action Fraud/NFIB Protect

In July we ran the social media phishing campaign #Reportthephish. This campaign reached a potential audience of 8,434,856 individuals, achieving 35,232,810 impressions. The week following the launch of the campaign the number reports to SERS increased by 27% to 148,520 reports. Although this decreased the following week to 135,906 reports this is still 16% higher than those reported the week before the campaign launched.

The reason behind the increased social media reach during the month of September can be attributed to posts from London Mayor Sadiq Khan and E L James (Fifty Shades of Grey author). This related to raising awareness of cost-of-living related scams.

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

Lead Force Operations Room

During Q2 2022-23, LFOR did not co-ordinate any National intensifications. This period is not favourable for such campaigns due to high abstraction rates over the summer months. However, during this period LFOR in partnership with the NECC and other agencies developed a number of intensifications that will take place in Q3. These will focus on Investment Fraud, Money Laundering linked to fraud and a National response to an investigation originating in the MPS.

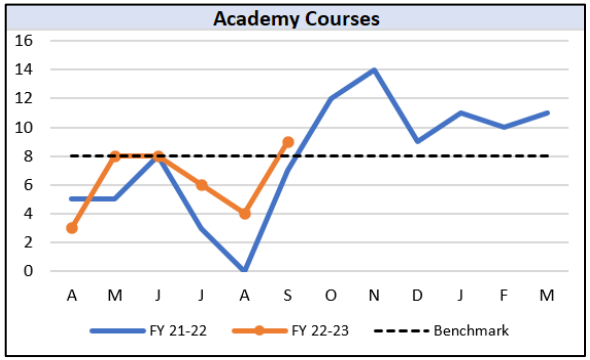
LFOR continue to work with CRIMESTOPPERS regarding the National Courier Fraud campaign. This is a 12 month intensification delivering PROTECT messaging to established networks. Latest NFIB figures show Courier Fraud reporting is down 60% on this time last year.

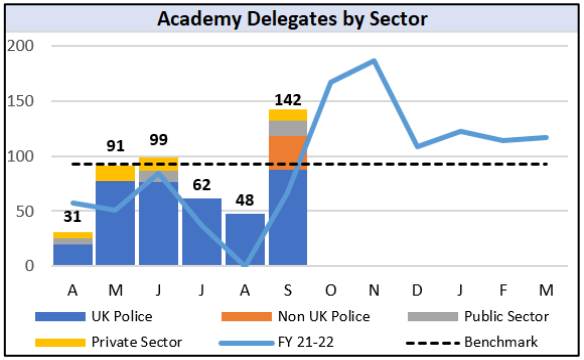
Outcome 5: *Building Capacity and Capability.*

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

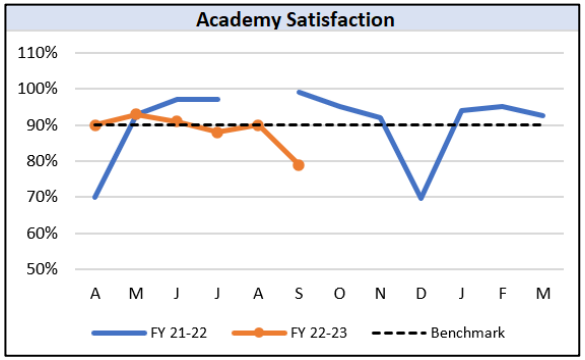
The Academy delivered two Money Laundering courses and a Victim Care Course to the NCA in July. Other courses delivered included Specialist Fraud Investigator and Bribery courses, along with Virtual Currency Courses attended by CoLP officers and staff. We also delivered an external MOD SFI course. In September the Academy were overseas in Serbia delivering courses to the Serbian Anti-Corruption Agency and Serbian Border Force. This training was aimed at investigators involved in dealing with corruption within the public sector. Other Academy activities included a CPD event on the Fraud Investigation Model (FIM) which attracted 466 attendees.





The ECCA delivered 19 training courses in Q2 which is consistent with the previous quarter and an improvement on the previous year as courses were run during August. However, the number of delegates almost doubled, and the courses provided were longer and more in-depth. The plan to increase the number of courses during Q2 was impacted by external factors such as train strikes and the Queen's funeral.

Delegate numbers are also increasing, and the Academy now has a better booking system which ensures no spaces are left empty. The number of delegates also increased throughout the quarter. 79% of delegates were from UK policing, with 12% from overseas policing.



Satisfaction averages fell slightly to 86% for the quarter. Although mostly positive, feedback evaluation has shown that a single feedback form has reduced the scores and was not indicative of the wider group experience. It has also been noted that only 48% of feedback forms were returned during the quarter, and improvement is required to ensure that all delegates are completing the forms.

Outcome 5: *Building Capacity and Capability.*

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

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

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

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

- The work of the **Intelligence Development Team** and their partners over the last three years has delivered huge success, especially with romance and courier fraud as part of the Project Otello campaigns. They continue to host national surgeries for law enforcement to share knowledge and issues, and to come together to tackle fraud. Other work includes Op Henhouse a national fraud campaign, and Op Haechi, an international fraud collaboration with Interpol. They are also currently working with the new Proactive Economic Crime Teams (PECT) across the regions for fast time pursue work on organised fraud crime
- Following evidence-based research, **financed by Lloyds Banking Group**, we licenced demographic segmentation data to better understand previous victims of fraud/cybercrime and thus identify chronic hotspots of victimisation. This means we can forecast potential victimisation by location, allowing forces the opportunity to conduct bespoke crime prevention outputs – an improvement to the one size fits all product previously completed. We now are working with 9 forces, delivering packages for Protect work in the hotspots we have identified, tailored to victims, with demographic data.
- The new **Enhanced Cyber Reporting Service** (ECRS) is providing a better service to business victims of cybercrime. The intel team are harnessing national Police Cyber Alarm data to understand the true threat to UK businesses from cyber attacks and attempts. The wider service will give a much more tailored and supportive approach to businesses which is then complimented by the wider cyber network, such as cyber resilience centres.

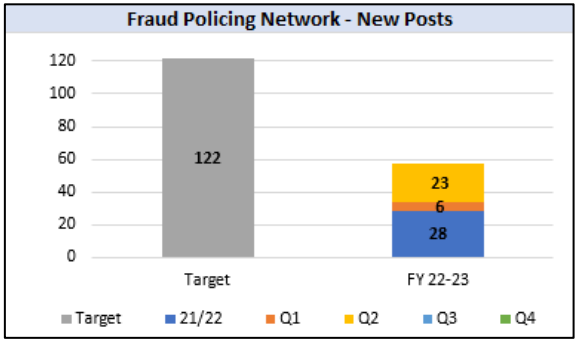
Outcome 5: *Building Capacity and Capability.*

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

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

Establishment of a new Fraud Policing Network (PURSUE) :

- Four proactive Economic Crime Teams (PECT) were established in four Regions during 2021-22 (Eastern, NW, West Mids, and Yorks & Humber). There has been a reduction of 1 post to 27 Police Uplift Programme (PUP) funded) police officers in post since Q1 due to a resignation in one Region.
- A further six Regional PECTs are to be established in 2022-23 along with enlargement of the existing PECTs. By the end of 2022-23 the target is for the network to have 122 staff (through PUP and Spending Review Funding) across 10 Regions and CoLP NLF. At the end of Q2, 57 posts are in place (47%).
- The recruitment of five new posts into the NFIB Intelligence Development Team has been completed. These posts develop intelligence packages for the Regions and NLF, and support the tasking and coordination of cases across the Network.
- The Network performance framework in place, with ongoing refinement.



Additional recruitment and retention strategies currently being realised include:

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

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 RAG assessment for the relevant measure.

Table 1 – Success Measure Performance RAG assessment	
OUTSTANDING	Performance consistently exceeds expected success measures
GOOD	Performance consistently meets expected success measures
ADEQUATE	Success measures have not been consistently met but plans are in place to improve by the end of the period
REQUIRES IMPROVEMENT	Success measures have not been consistently met and there is insufficient evidence that performance will improve by the end of the period
INADEQUATE	It is unlikely the success measures will be met for the annual period based on the quarters to date
NO GRADING	Insufficient evidence means that no meaningful assessment is possible at this time

This page is intentionally left blank

Committee(s): Economic and Cyber Crime Committee	**Dated:** 25 November 2022
Subject: National Lead Force (NLF) Update	**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 108-22	**For Information**
Report author: DI 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:

- Tackling Economic Crime Awards
- NFIB developments
- Key investigation outcomes
- National Police Chiefs Council (NPCC) Update

Recommendation(s)

Members are asked to note the report.

Main Report

Background

The National Lead Force Plan was approved by Police Authority Board in October 2020. Detail was given around new plans at the previous ECCC in September and further updates in October. This ECCC is much closer than usual to the previous committee and so updates necessarily shorter in length than would be usual. The new performance measures are now in place and present on the accompanying performance 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.

Next Generation service project update

The Fraud and Cyber Crime Reporting and Analysis System (FCCRAS) Procurement Committee approved the Procurement Recommendations for FCCRAS on Wednesday 2nd November. Further approvals are progressing.

Action Fraud

Action Fraud are thrilled and honoured to have been nominated for three awards in the upcoming Tackling Economic Crime Awards (TECAs). The TECAs are designed to recognise excellence and innovation in tackling all areas of economic crime from those working in the private, public and third sectors. Winners of the 2022 TECAs will be announced mid-November (post submission date) at a gala dinner and ceremony due taking place at the London Marriott Grosvenor Square.

NFIB

- National Fraud Intelligence Bureau (NFIB) crime assessment team has rolled out a new vulnerability assessment tool. This better identifies those victims of fraud and cyber-crime who are more vulnerable due their age (juveniles); or because their report indicates a link with domestic abuse (DA) or stalking or harassment (SH).

- The NFIB cyber team has also made improvements to their Enhanced Cyber Crime Reporting Service (ECRS), reducing the time taken to review and disseminated all business related reports made to Action Fraud reports, from 7 days to 72 hours.

- On Tuesday 15th November the first phase of the Action Fraud Christmas campaign was launched alongside with the National Cyber Security Centre (NCSC), focussing specifically on online shopping safety in the run up to Black Friday and the festive season. The NCSC and Action Fraud are issuing joint press releases, to help drive awareness and engagement around shopping safely online. The release uses data from the Action Fraud / NFIB online shopping report as a compelling hook for the media. A social media schedule containing protect messaging and assets have been developed to support the campaign and will be circulated to partners and forces. The online shopping activity precedes Action Fraud's annual '12 Frauds of Christmas' campaign which is due to launch at the beginning of December.

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.

NFIB

DCS Shaw met with representatives of OFCOM which is currently researching protocols that will support the Online Safety Bill when enacted.
OFCOM is particularly interested to understand NFIB's disruption work (with a focus on technology platforms and TELCOs). Further, there is a joint concern around the willingness of some platform providers such as Meta to engage in entity removal (e.g.

accounts / specific pages). This meeting was seen as the first stage of a regular dialogue – in preparation for the launch of FCCRAS in 2024.

Outcome 3: Investigate and Prosecute.

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

PIPCU - Operation Heartbeat

Warrant executed in Southall, West London. Approximately 84,000 counterfeit items seized. Estimated value to industry is £200m. The watches were destined to supply criminal businesses all over the UK. This has seriously disrupted the counterfeit watches trade in the UK in the lead up to Christmas. Ongoing work continues to dismantle the OCG that sits behind the criminality.

National Lead Force

Op Corona - Conviction of 4 suspects in Op Corona. This was an investment fraud with 343 victims who were all supported to an exceptionally high standard by the Victim Care Unit (VCU). The Police Staff Investigator received a Judges Commendation ' in recognition of the high-quality work completed in bringing this case to court'.
In this same period a high-profile trial has begun, this is Op Adonis. This is an investment fraud prosecution centring on high-risk high-reward Binary options trades. There are 172 victims with a combined loss of £2.2M.

DCPCU - Operation Quinn

A Nat West bank related courier fraud. The team executed a warrant in Tower Hamlets and found a single subject alongside £100k in cash kept in a cardboard box in a wardrobe. Hundreds of thousands of pounds of designer clothing and goods which had been purchased using compromised details from victims were also found and seized. On 9th November 2022 the defendant was sentenced to a total of 2 years 6 months imprisonment, having pleaded guilty to all offences.

IFED

On 9th November 2022 three warrants were executed by IFED around the UK. This stemmed from a false motor insurance claim, valued at over £40k. At the time of the incident one of the suspects was a serving officer with West Midlands Police.

Outcome 4: Raise Awareness and Prevent Crime.

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

NLF – The Operation Broadway (Investment Fraud) intensification campaign ran into November and there was successful engagement with businesses and serviced offices to educate not only other serviced offices and other enablers of investment fraud but also to the public.

NFIB – The Christmas online shopping campaign launched on the 14th November. This work has included the National Cyber Security Centre and uses social media, websites and radio output. This campaign has used research to give targeted online Christmas shopping advice to help consumers avoid falling victim to scams.

DCPCU – The security minister, Tom Tugendhat MP MBE has requested a visit to DCPCU and this is likely to occur in November. Full details awaited at time of writing.

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.

National Police Chiefs Council (NPCC)

DCS Andrew Gould gave evidence to the Parliamentary Economic Crime & Corporate Transparency Bill Committee on 25th October in relation to its cryptocurrency provisions. We are supportive of the Bill and many of the new powers are there at our request.
National Cybercrime Governance Board was held on 25th October with all the Regional Chief Officer SROs. Discussions focused on the HMICFRS Recommendation and options for NPCC.

On the 10th October the Cyber Resilience Centre network summit was hosted at Microsoft in London. This brought together the full team of national Cyber Ambassadors, these include KPMG, Cantrum, CGI (cyber security advisors), Accenture, Very Group, Natwest, Chainalysis and Microsoft. Also present were Cyber Resilience Centre leads and the national cybercrime programme team.

This was a very successful day and brought the network together for the first time as a whole and plans for the future were workshopped.
Each ambassador has now taken leadership to deliver an area of the plan and working groups have been established to progress the work.

The London Cyber Resilience Centre had its public launch at City Hall on the 25th October. Commissioner Angela McLaren and Mr James Thomson, Chair of the City of London Police Authority Board, spoke at the event alongside the Deputy Mayor for Crime and Policing in London. The event was judged a success with a number of companies coming forward to support the centre and more work will be done to build upon this launch.

National Coordinator's Office

Visits around the country continue in this period,
Fri 4th Nov –Chief Officer engagement with Devon and Cornwall
Mon 7th Nov – Force Engagement with Surrey and Sussex
Mon 7th – Chief Officer engagement with Avon and Somerset

Economic and Cyber Crime Academy - ECCA

Representatives of the ECCA [Academy's] attended a HMICFRS round table workshop with Commander Nik Adams and Detective Supt Fraud Operations regarding fraud and training across the UK.

Academy representatives attended a knowledge sharing event regarding neurodiversity run by the College of Policing and Chaired by Vanessa Jardine, Deputy Chief Constable of West Midlands Police, and lead for Diversity & Inclusion in Armed

Policing. This was an opportunity to understand the National picture in regard to neurodiversity and a chance to introduce the Academy new neurodiversity course, being run by the Academy for the City of London Police in partnership with the NPCC Cyber Team.

Detective Chief Inspector for the Academy chaired a meeting with Directorate DCI leads to ensure that the newly design pathway for Police Staff Investigators would be able to secure cross unit pollination and learning. For PSIs to become qualified to PIP2 (Professionalising Investigation) level there is a need for those staff, like the Detective pathways, to move around on short attachments to learn all key areas of business. A pilot training model will now be implemented and lead by the NLF Fraud team.

Proactive Economic Crime Teams (PECT)

Recruitment is on-going and the teams are up and running. A current status update on recruitment is as below;

TOTAL ROCU & CoLP Police Uplift Programme & Spending Review	Recruited 2021-22	Target 2022-23	Recruited 2022-23	% 2022-23 Target Achieved (To end of financial year)
Total Officers	29	122	59	48%

There is confidence that targets will be met. In most regions recruitment is going very well and a number of posts are at the vetting stage or awaiting start dates.

The total case load so far is 126 cases, 82 are self-generated by the PECT teams and 46 were assigned from the City Police Intelligence Development team. the Eastern region are performing especially well in terms of PURSUE and Yorkshire and Humberside have seen some good early work on low level disruptions. It is hoped work will build rapidly over the coming months.

Contact:

Kevin Ives
Detective inspector
Staff officer
E: Kevin.ives@cityoflondon.gov.uk

This page is intentionally left blank

Committee(s): Economic and Cyber Crime Committee	**Dated:** 25 November 2022
Subject: Quarterly Cyber Griffin Update	**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 109-22	**For Information**
Report author: Charlie Morrison, Detective Inspector, Cyber Griffin, Specialist Operations	

Summary

After experiencing a levelling-off of service over the summer period due to wider policing demands, interest in Cyber Griffin's more scalable services is returning. It is not yet clear whether this period of high demand will place Cyber Griffin back on track to hit the programmes new, higher annual delivery targets however the programme is confident in achieving its Q3 targets. The unit remains one officer understrength. The programme's duty to provide security advice and guidance within the Square Mile will remain its priority and resourcing will be closely monitored to ensure this objective is met.

Recommendations

It is recommended that Members note the report

Main Report

Introduction

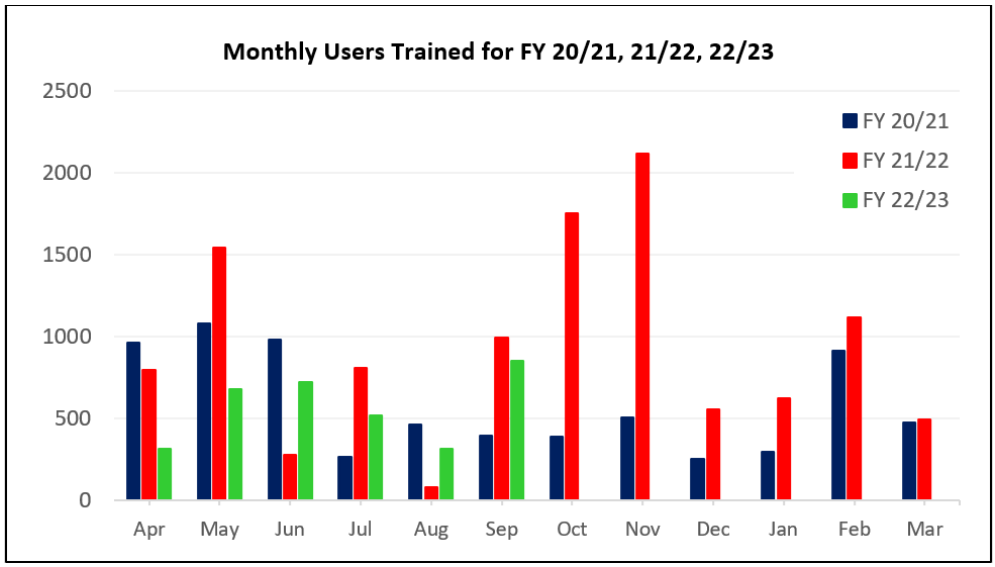
1. This report will give a brief update on the current position of the Cyber Griffin programme. For details of all Cyber Griffin services please visit: www.cybergriffin.police.uk

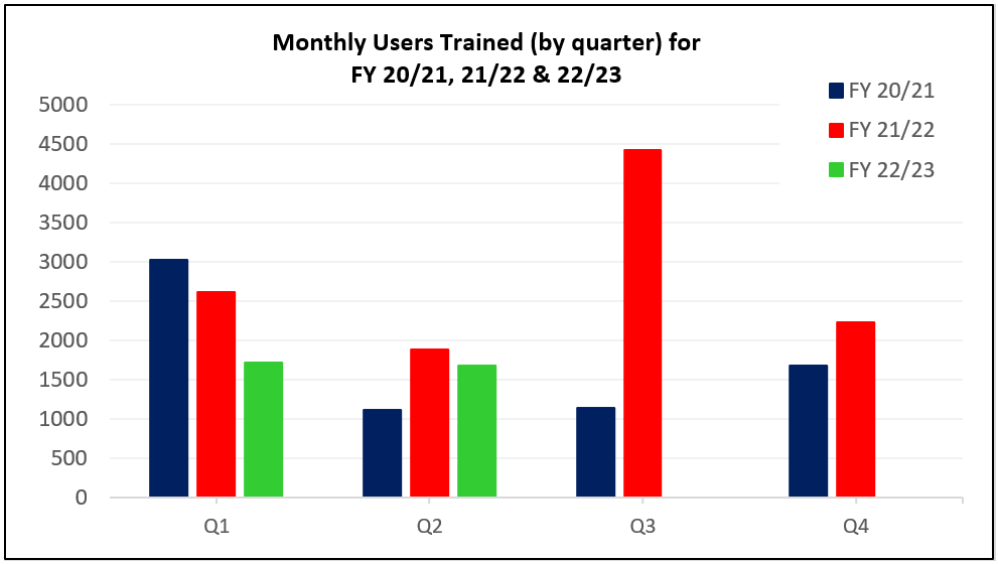
Current position

2. Cyber Griffin's performance, as predicted, was lower in Q2 than in previous financial years. This was in part due to a high level of abstractions and a shift in the community's

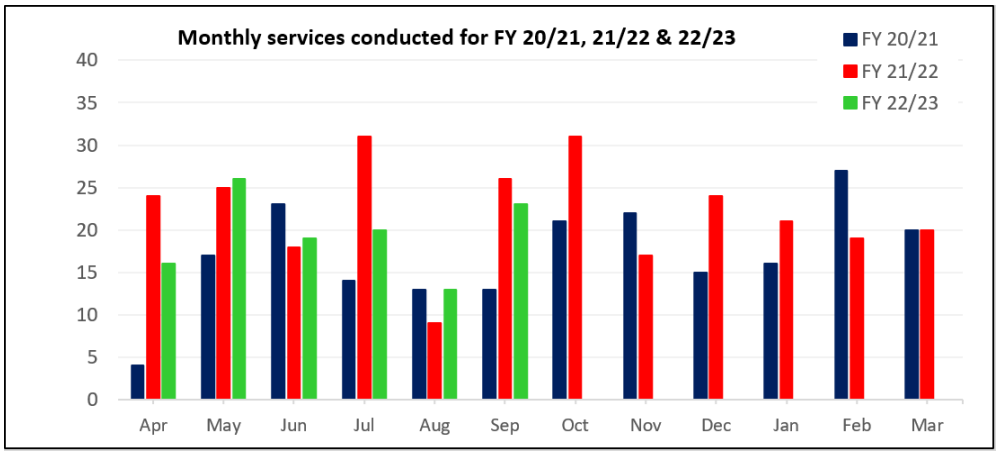
interest towards Incident Response Training and Cyber Capability Assessments. These services, whilst extremely valuable, place a greater demand on officer time and involve fewer participants meaning they impact performance statistics negatively when compared with Cyber Griffin's other services. It should be noted in relation to these services, that survey responses monitoring an organisation's behavioural change have been extremely high. As Q2 closed, the programme has already begun to see a large increase in demand as well as a more balanced request across Cyber Griffin's four core services. While it cannot be reflected in this quarter's return, the programme is now experiencing a very high level of demand which is making up for a challenging summer of disruption.

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





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



3. Regarding locally set targets, the more ambitious annual targets set for Cyber Griffin remains challenging but achievable if the uptake in service demand continues. The programme trained 1,687 people (quarterly target of 2,500), conducted 56 services (quarterly target of 67) and partnered with 39 new client organisations (quarterly target of 36) in Q2.

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 performance, Cyber Griffin is forecast to go through a high demand period. October has already broken previous yearly performance records and November also looks very positive. What is clear from this financial year, is the importance of Cyber Griffin's visibility to the public. Speaking at Security Summits and gaining the public support of key members of the community has invariably been followed by peaks in service requests. Data shows, that Cyber Griffin retains a long-term relationship with the majority of organisations the programme engages with. This is an encouraging indicator of value and demonstrates the importance of making a first contact. More effort will be focused on this area of business in the next quarter.

6. Cyber Griffin's financial situation is extremely positive. The programme has confirmed both the Corporation Business Levi and NPCC Cyber Crime Programme funding. Combined with the unit's current funding (due to end in April 2023), Cyber Griffin has stable long-term funding going forward. Discussions with senior officers as to the next stage of the programme's development remain ongoing. The central aim, as always, is to provide long-term impactive digital security for the Square Mile.

7. Cyber Griffin continues to work with Bristol University in the development of a new Incident Response Exercise. What separates this training from alternatives, is that

Cyber Griffin will be offering an ‘open world’ exercise. This means that participants will be able to use the exercise multiple times to sharpen their incident responder skills. The exercise is now reaching its testing phase; initial feedback is extremely encouraging and roll out is expected next year.

8. Finally, the protect advice landscape in London has changed with the launch of the London Cyber Resilience Centre (CRC). This is a not-for-profit ‘cyber protect’ advice initiative supported by policing and the Home Office. Cyber Griffin remains in contact with CRC leads and is supporting the initiative in establishing itself in London’s communities.

Conclusion

9. Cyber Griffin continues to offer a very well-regarded and effective cyber security programme. After a challenging Q2 which saw a drop in performance, the programme is now recovering this lost ground in a very strong start to Q3. The unit observed the impact of increasing the programme’s visibility on service delivery and a greater focus will be placed on this over the next period.

Contact:
Charlie Morrison
Detective Inspector
Cyber Griffin
Specialist Operations
E: Charlie.morrison@cityoflondon.police.uk

Committee(s): Economic & Cyber Crime Committee	**Dated:** 25/11/2022
Subject: Innovation & Growth – Update of Cyber & Economic Crime related activities	**Public**
Which outcomes in the City Corporation's Corporate Plan does this proposal aim to impact directly?	1, 6, 7
Does this proposal require extra revenue and/or capital spending?	No
What is the source of Funding?	**NA**
Report of: Damian Nussbaum, Executive Director Innovation and Growth	**For information**
Report author: Elly Savill, Policy and Technology Adviser	

Summary

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

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 on October 3rd 2022. The report focuses on a detailed update on how CoLC and CoLP plan to jointly deliver the upcoming Cyber Innovation Challenge 2.0.

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.

<u>Collaboration</u>

3. On Saturday 15th October the City of London hosted The Golden Key, agree, immersive event which aimed to boost footfall to the area and support the City

visitor's economy. The initiative was led by IG's Destination City team with ongoing support from CoLP who regularly attended The Golden Key Licensing, Operations, Safety & Planning Group (LOSPG) during the planning stage of the event. CoLP also shared intelligence with CoLC on the possibility of protests on the day and provided a contact within the City Police control room to ensure the event ran smoothly.

Promotion of CoLP activity

4. During October, the Lord Mayor highlighted the importance of protecting the FPS sector by ensuring a strong defence against cybercrime at events including the breakfast with Members of the Royal College of Defence Studies, Lord Mayor's Defence and Security Lecture and Worshipful Company of Security Professionals' Dinner. As part of this, the work of CoLP was highlighted.

5. At the end of November, the 2022-2023 Lord Mayor Nicholas Lyons will visit Cardiff as one of his first domestic visits in the Mayoralty. This will include engagement on the newly invested-in Cyber Security Innovation Hub which is central to the South Wales Cyber Security Cluster. The aim of this visit will be to build out discussions around opportunities for investment and mentoring, skills development and start up acceleration. However, this visit could also provide an opportunity for the Lord Mayor to highlight CoLC's close working relationship with CoLP and their role as the national policing lead for cyber.

Innovation & Growth activity

Cyber Innovation Challenge 2.0

6. In the last update the Committee was informed that the CoLC and CoLP were in the process of agreeing a project plan for a second Cyber Innovation Challenge to be delivered in partnership by both institutions. A detailed project plan has now been agreed and can be found in the Annex. The strategic outcomes of this new cyber project would be to:
    a. Accelerate development of innovative cyber-security solutions that meet FPS and wider relevant industry demand;
    b. Support cross-sector collaboration and information/data sharing on an emerging and/or key cyber-security challenge; and
    c. Provide thought leadership on catalysing cyber innovation in the UK.

7. The Challenge supports the wider joint aim of CoLP and CoLC to support a thriving economy by ensuring the UK is the most secure place globally for Financial and Professional Services (FPS) to do business. To achieve this, the project will identify a key cyber challenge facing FPS and wider relevant industry and provide a unique opportunity for industry and tech companies with innovative solutions to collaborate over a six week sprint to develop technologies to address the use case. We anticipate the Challenge will run for twelve months (more detail below).

8. The early stages of the project will commence in Q4 2022 and run until the start of Q4 2023. CoLC will assign a Policy and Technology Adviser to lead on the delivery of the project and will cover the whole cost of the programme, which is

estimated at £20,000. CoLP and CoLPA will jointly resource the challenge, having already identified individuals to be the relevant leads on delivering various phases of the Challenge.

9. The project plan includes multiple phases of work taking place across a 12-month period. A summary of four key phases of the project is set out below.

10. **Initial partnership discussions**
The end of Q4 2022 into Q1 2023 will centre around identifying potential third party partners for the Challenge. This is likely to be a mixture of 'founding' partners who are involved in the day-to-day activity of the Challenge and 'supporting' partners who assist with delivery, but are less actively involved. CoLC and CoLP will both suggest possible partners. These might be existing contacts, bring specific strengths such as cyber expertise, have been previously involved in the Challenge (e.g. Microsoft, DIT, London and Partners) or be an opportunity to build a new stakeholder relationship. Last month IG engaged with Microsoft who confirmed an interest in being involved in the second iteration of the Challenge.

11. **Agreeing the Challenge use case**
A critical stage for Q1 2023 will be to identify the use case on which the Challenge is based. This will be a current, likely high risk issue facing FPS and wider relevant industry. The input of CoLP will be a particular strength during this stage, as they will be able to draw on internal knowledge and intel on relevant emerging cyber-security challenges. Meanwhile CoLC will utilize existing stakeholder relationships within FPS to identify top cyber-security challenges facing the sector.

This joint intelligence will be discussed and built out through workshops hosted by CoLP, CoLPA and CoLC with representatives from the FPS and cyber sectors as well as Challenge partners. These workshops will also provide an opportunity to identify an initial pool of possible FPS and industry participants to approach.

12. **Industry participant confirmation and technology participant applications**
Following the confirmation of the use case, Q2 2023 will focus on identifying both the industry and technology participants. Although delivered alongside one another, these are two stages that will require different processes of engagement. When making initial approaches to potential industry participants, the scope and objectives of the Challenge as well as the time commitment required will be made clear. Technology companies on the other hand, will be identified via an application process. The first Challenge used the Digital Sandbox Platform for this, however a new process for submitting and assessing applications will be designed.

13. **Challenge delivery**
Following the confirmation of industry and tech company participants, the sprints will take place in Q2-Q3 of 2023 in the form of a range of set events. Separate check ins with participants will also be held to gather feedback which will benefit the evaluation report.

14. **Evaluation**

The final stage of the Challenge will be the publication of the evaluation in early Q4. The evaluation will measure the effectiveness of the Challenge, how it has met its objectives and the key takeaways. Measurements will likely be based on those used for the previous evaluation which included collaboration, impact on innovation and market facing impact.

Conclusion

This project reinforces shared interests of CoLC and CoLP and provides an excellent opportunity to draw on our respective industry and government contacts, and share insights and expertise to support FPS and wider industry to protect against emerging cyber threats.

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

CoLC/CoLP Cyber Innovation Challenge– Project Plan

Introduction

In 2021 the City of London Corporation (CoLC) and Microsoft partnered to develop an Innovation Challenge bringing together the financial and professional services (FPS) and tech sectors. Cyber security was selected as the theme for the Challenge with a focus on technology to support assessing, continuously monitoring and mitigating risks across the supply chain. The primary aim of the Challenge was to foster collaboration between financial institutions and technology companies. Specifically, the Challenge was designed to:

(i) Cut across silos between traditional sectors and revitalise the ecosystem;
(ii) Challenge organisations to work together on defining and solving a widespread problem statement; and
(iii) Use the opportunities afforded by the Challenge, including the Digital Sandbox platform, to accelerate tech development so that it is market ready.

The Cyber Innovation Challenge involved financial services institutions engaging in weekly meetings with tech companies who were selected for the Challenge via an open application process. During this six-week sprint participants had focused conversations to explore the solutions and how they could be developed to better meet the needs of the FPS sector. The tech companies also attended collaboration sessions to provide them with further insights from across the cyber security eco-system. The Challenge culminated in a final presentation session bringing together all the participants. This provided the technology companies with a chance to present their solutions and explain how they had developed due to participating in the Challenge.

An evaluation of the Challenge has demonstrated positive results. In particular, it confirmed that the Challenge represented a new offering to the market and that levels of engagement from the FPS sector and collaboration between participants to the Challenge were positive. Successful outcomes include pilots that are now being conducted between some of the tech companies and the FPS partners, improvements in the solutions that have been made because of the discussions that took place and partnerships between the tech companies themselves. All those involved in the Challenge who responded to a survey confirmed that they would recommend participating in the programme. All tech companies who completed the survey also confirmed that their involvement in the Challenge accelerated product development.

Cyber Innovation Challenge 2.0

Background

FPS and related sectors remain some of the most targeted sectors for cyber-attacks and these threats are constantly evolving as bad actors develop new methods for advancing cyber threats. As the forms of attack become more innovative, there is an ever-increasing need for more innovative solutions aimed at these markets. There are many who are already working hard to develop products in this area. These range from across the FPS sector, BigTech and other fintech and cybertech specialists. However, there is significant scope to bring better products to the FPS market and wider relevant industry more quickly by supporting collaboration across these sectors. Both CoLC and Microsoft have already indicated an interest in responding to this opportunity by developing an enhanced version of the Cyber Innovation Challenge.

As the national policing lead for cyber, the City of London Police (CoLP) plays a significant role in helping to build a resilient and secure eco-system in which both individuals and businesses across the UK can operate safely. CoLP has a unique insight into the cyber-security challenges that businesses face on a day-to-day basis. CoLP also has information on emerging trends in this area and their potential impact on the business community. This creates an opportunity for CoLC and CoLP to partner on delivering a Cyber Innovation Challenge that will strengthen the UK's cyber security credentials by combining CoLP's strengths as national policing lead for cyber with CoLC's industry and innovation networks and capabilities. A key role of CoLC will be to draw upon its prior experience of running Innovation Challenges of this nature to inform the format and delivery of the Challenge in a way that will be successful. CoLP's primary role will be to provide cyber security expertise and knowledge of both the cyber-security threats and solutions already available in the market. This will be vital to setting the use case, recruiting participants and ensuring that the Challenge is relevant to the FPS, wider relevant industry and tech sector participants that it is aimed at. The primary risk for both parties is advancing a Challenge that will have limited impact on the market and so ensuring that the underlying theme for the Challenge and the format in which it is delivered appeals to the FPS sector is key. Both CoLC and CoLP will have a complementary role to engage their business and broader networks in the Challenge to mitigate this risk.

The Cyber Innovation Challenge advances the CoLC corporate strategy objective to support a thriving economy. It also links to Innovation and Growth's specific business plan objective to ensure that the UK's financial and professional services are at the forefront of tech adoption and innovation. Specifically, the Challenge will support tech to scale by taking innovative solutions that are either at the early stage of development or require support to pivot to the FPS sector to scale. The Challenge supports the City of London Policing Plan priority to protect the UK from economic and cyber crime and builds on its collaboration with industry to improve cyber resilience (National Cyber Resilience Centre Group Ambassador Programme), and share intelligence. This is an objective of both CoLP and CoLPA.

Objectives

The overarching objective for this joint project between CoLP and CoLC is to strengthen the UK's cyber security credentials. In doing so the project should focus on achieving three core aims:

1) Accelerating development of innovative cyber-security solutions that meet FPS and wider industry demand;
2) Supporting cross-sector collaboration and information/data sharing on an emerging and/or key cyber-security challenge (including between industry and policing); and
3) Providing thought leadership on catalysing cyber innovation in the UK.

To achieve these objectives, the Challenge must engage with individuals and organisations from across industry, cyber and tech sectors as well as regulators and government departments operating in the cyber security space. Depending on the use case selected for the challenge there may also be a need to involve data providers, cloud service providers and other areas of law enforcement.

In terms of the project's KPIs, there is scope to draw upon the success criteria that were developed from the previous Microsoft Challenge. In particular, the following are likely to be relevant to the Cyber Innovation Challenge:

1. Market Facing Impact – Proof of accelerated/new product development resulting from the Challenge and the potential for these products to impact industry participants including the FPS market. This will draw upon feedback received from tech participants on the Challenge's role in supporting product development and marketing of their solutions. Any input from industry participants on plans to test and/or integrate any of the solutions coming through the Challenge will also be relevant to demonstrating that this objective has been met.
2. Involvement of key sector representatives including FPS – Numbers and breadth of representation at all stages of the Challenge development and delivery. This is key to ensuring that the Challenge is relevant to the sector and is in the best position to positively impact industry and FPS response to cyber security threats.
3. Collaboration – Evidence of collaboration between different participants in the Challenge. There is a focus on how the industry and tech participants work together (as demonstrated through number of sessions held, feedback provided etc), but it is also important to factor in collaboration with the broader cyber-security eco-system and between tech participants and/or industry/FPS participants themselves. This all has the potential to help improve the understanding of and response to cyber security threats.
4. Thought Leadership - Demonstrating that the Challenge is meeting a need not already being resolved within the market. This can be reflected in the topical and unique focus of the use case underlying the Challenge and/or the format of the Challenge which is not replicated through other groups or forums. This could also be demonstrated by reviewing the number of stakeholders engaged either through the Challenge itself or as part of the lessons learnt and knowledge sharing arising from it.

Project Plan

Fundamental to the successful delivery of the project is agreement between CoLC and CoLP to combine resources and commit to the work required. The following project plan sets out the proposed scope of work, timetable and initial responsibilities to be set between CoLC, CoLP and possible third party partners to the project. As noted above, Microsoft has already confirmed its interest in being involved and there is scope for exploring this and additional partnership roles to support the development and delivery of the Challenge.

	Timeline	**Phase of Work**	**CoLC Role**	**CoLP/CoLPA Role**	**Notes**
1	November 2023	**Confirmation of project plan**	To provide a suggested project plan for CoLP review and input	To provide substantive input into project plan and confirm agreement to committing time and other resource to delivery of the Challenge	Project plan to be signed off by Innovation & Growth SLT and CoLP and presented at ECCC November meeting for approval

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
2	December-January 2022	**Initial partnership discussions** – CoLC and CoLP to agree on a list of potential third party partners for the Challenge, clarifying their role and remit eg as experts, funders etc This is likely to be a mixture of 'founding' partners who are involved in the day to day activity of the Challenge and 'supporting' partners who assist with delivery, but are less actively involved. CoLP and CoLC will then work together to approach and recruit partners to the Challenge	To suggest other partners that could support delivery of the Challenge. This will include those that bring specific strengths on technology development, cyber expertise and data. This is likely to include previous Challenge partner Microsoft, but also possibly UK Finance, LORCA and others	To suggest other partners that could support delivery of the Challenge. This should include those organisations with which CoLP / CoLPA has strong ties including the NCSC and who weren't engaged with the previous Challenge, but could provide useful input	It might be sensible to limit the number of 'founding' partners to help align objectives. Microsoft were a valuable partner previously in terms of branding and providing input on cyber security theme, access to relevant industry/FPS contacts. Also worth considering at this early stage broader industry/government partners as were used before who support the Challenge, but are less involved in the day-to-day delivery
3	January-February 2022	**Challenge objectives and evaluation framework agreed** – CoLC and CoLP to agree a set of key objectives for the Challenge and refine with partners to ensure that measures of success are clear and agreed from the outset	To table CoLC objectives expanding on those set out above and taking into account those adopted for the previous Cyber Innovation Challenge	CoLP to ensure that its own objectives are clear and being met as a result of the work to be undertaken across the Challenge	This objectives setting should include agreement of KPIs and how the success of the Challenge will be measured. This includes consideration of how any data will be captured to support the evaluation eg entry/exit surveys from participants
4	January-March 2022	**Challenge use case setting** – it's integral that the Challenge addresses a key cyber-security issue that is being faced by businesses. Initial input on possible topics should be explored by CoLC, CoLP and	To provide initial input on possible use case from stakeholders (via existing contacts/SRM) on top cyber-security challenges being faced by FPS. To organise workshops including proposing attendees	To provide input on possible use case from internal knowledge and intel on emerging cyber-security challenges being faced by relevant sectors. To propose attendees, and jointly agree	In terms of the workshops it would be useful to consider the use cases from three different perspectives: (i) relevance/impact on FPS/relevant industry; (ii) capability for tech solutions to respond to the challenge; and (iii) blockers to

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
		other partners before bringing in wider stakeholders from across industry/ FPS and cyber sectors in a series of workshops to discuss and refine an agreed use case	and jointly preparing agenda and leading discussions with CoLP	agenda and leading discussions with CoLC	solutions reaching market eg is there a data issue etc Workshops to include input from both the FPS and cyber/tech sectors
5	March-May 2022	**Challenge timetable development** – a timetable and programme of activity for the Challenge needs to be agreed. This is likely to include 1:1 feedback sessions between industry/FPS/tech participants, wider collaboration/learning sessions, data provision/creation and a public showcase event	To provide information from previous Cyber Innovation Challenge on format adopted and feedback from evaluation report on lessons to be learnt for any future iterations of the programme. Can also seek input from previous participants if helpful	To provide input on how CoLP may be able to support on different aspects of the Challenge eg any relevant data sources that CoLP holds which could be shared as part of supporting the development of tech solutions coming into the challenge	Collaboration between industry/FPS and tech participants is at the core of the Challenge programme. However, depending on the use case selected it would also be good to explore whether there is potential to provide tech participants with access to data or other support that they may need to accelerate development of their solutions
6	April- May 2023	**Industry participant confirmation** – once the use case has been finalised and the Challenge timetable set industry/FPS participants should be approached to take part. Their role will be to work with the tech companies to help them develop their solutions to meet the needs of their respective organisations and broader sectors	To make joint approaches with CoLP to potential industry participants confirming the scope and objectives of the Challenge as well as the time commitment required	To make joint approaches with CoLC to potential industry participants confirming the scope and objectives of the Challenge as well as the time commitment required. This is an opportunity for CoLP to engage with key business contacts eg Cyber Ambassador network	The use case workshops should provide an initial pool of possible industry/FPS participants to approach. There will need to be clarity up front of what time commitment is required and when to ensure that they are able to commit and participate fully

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
7	April-May 2023	**Technology participant applications** – to run an application process for technology companies that want to submit solutions into the Challenge. There should be clear eligibility and other criteria against which these will be assessed and a panel constituted to reach a decision on which companies to bring into the Challenge	To provide input on process and potential criteria for assessment from previous Challenge. To draft and publish call for applications and share across networks. To assess applications and inform applicants of outcome	To input on proposed process/criteria for applicants based on CoLP knowledge of cyber security solutions currently in the market. To draft and publish call for applications and share across networks. To assess applications and inform applicants of outcome	Whilst the Digital Sandbox platform was used for the application process previously, it will not be available for this Challenge. A new process for submitting and assessing applications will need to be explored
8	May 2023	**Challenge finalisation** – once all participants are confirmed the programme of activity for the Challenge can be finalised. This will include final scheduling of sessions with all industry/tech participants and any other partners who will be involved in delivery of the Challenge	To confirm final scheduling and features of the Challenge (eg access to data, collaboration sessions etc)	To confirm final scheduling and features of the Challenge (eg access to data, collaboration sessions etc)	With the previous Challenge participants were required to agree to comply with Terms of Engagement. Consideration will need to be given as to whether this is sufficient or more formal Non-Disclosure Agreements are required
9	June-July 2023	**Challenge delivery** – the Challenge will be delivered through a set programme of events. This was previously run as a six-week sprint, but it would be sensible to explore different options for extending the timeframe of the Challenge and	To co-lead delivery of the Challenge including CoLC/CoLP/CoLPA representation at all sessions to guide discussions and provide any additional support required	To co-lead delivery of the Challenge including CoLC/CoLP/CoLPA representation at all sessions to guide discussions and provide any additional support required. To also consider CoLP leading a focused collaboration session	Regular check-ins should also be scheduled with all participants during the Challenge to gather and action feedback wherever possible. Based on previous experience, the Challenge should be timetabled to avoid public and/or school holidays wherever possible

	Timeline	Phase of Work	CoLC Role	CoLP/CoLPA Role	Notes
		building out the programme of activity		on CoLP activity in the cyber security space	
10	September 2023	**Public showcase event –** a public event to demonstrate the work undertaken within the Challenge and the solutions that have been developed as a result	To schedule event, confirm format, recruit participants and send out invites	To support on the delivery of the showcase event and help promote as appropriate	To consider any press release and/or marketing to be carried out through CoLC/CoLP channels to support the event
11	October2023	**Challenge evaluation published –** this report will provide further information about the Challenge as part of the thought leadership to be provided on driving cyber innovation in the UK. It will also demonstrate how the Challenge has met its objectives and/or what lessons can be learnt from its delivery	To draft report jointly with CoLP and arrange for publication and any related press release and marketing through CoLC channels	To review and agree report and promote through CoLP/CoLPA channels	

Resource

The Cyber Innovation Challenge should be viewed by both CoLC and CoLP/CoLPA as a significant project. Time and cost resource needs to be committed by both partners. The likely time resource required from both CoLC and CoLP/CoLPA is around 2/3 days per week from November 2022 – October 2023 increasing up to at least 4 days per week from January 2023. The estimated resource cost is £20,000 and will be covered by CoLC. There is potential for further costs to be incurred in developing and sharing data sets for the Challenge, but this will depend on the use case selected and the support sought by the tech companies participating in the Challenge to develop their solutions.

CoLP/CoLPA will jointly resource the challenge. Det Supt Martin Peters and Det Chief Supt Richard Waight will provide strategic leadership and contribute to the discussions on partners and development of the use case. They will consider involving other experts (such as the CoLP Director of Information Security)

in development of the use case. They will be supported by Helen Thurtle who will be the key point of contact for CoLP attending project team meetings and participating in the challenge delivery workshops. The CoLPA project lead will be Oliver Bolton who is responsible for cyber-crime policy and partnerships.

This can be broken down as follows:

Timeline	Phase of Work	Estimated Time Resource	Estimated Cost
November 2022-August 2023	Throughout project	Weekly project team meetings (30/45 min meetings) to share updates, check progress against project plan and milestones and progress any actions or decisions..	N/A
November 2022	Confirmation of project plan	- Review of project plan and meetings to refine the doc (4 hours[1]) - Finalising project plan and presenting for any CoLC/CoLP internal sign-off including joint presentation at the September Economic & Cyber Crime Committee (6 hours)	N/A
December 2022-January 2023	Initial partnership discussions	- Partnership brainstorm (60 min meeting) - CoLC to lead with support from CoLPA: - Preparing partner information pack on Challenge (4hours) - Scheduling/attending meetings with potential partners (12 hours) - Follow up with partners to confirm involvement and role (6 hours)	N/A
January-February 2023	Challenge objectives and evaluation framework agreed	- CoLC to lead with support from CoLPA: - Meetings re-evaluation framework (4 hours) - Gathering input from any other partners (4 hours) - Reviewing and finalising documentation (6 hours)	N/A
January-March 2023	Challenge use case setting	- Gathering input for possible Challenge use case (6 hours) - Initial CoLC/CoLP/CoLPA meetings re Challenge use case (4 hours) - CoLC to lead on organising use case workshops including scheduling, inviting attendees, setting agenda and preparing for workshops (12 hours) - Attending workshops and analysing input received (12 hours) - Final discussions and decisions on use case selection (6 hours)	N/A

[1] This is the likely time commitment required by each of CoLC and CoLP eg 4 hours of CoLP time plus 4 hours of CoLC time.

March-May 2023	Challenge timetable development	- CoLC/CoLPA meetings to develop Challenge timetable and features including 1:1 feedback, collaboration sessions etc (4 hours) - Exploring data asset relevance and availability to be included in support of the Challenge (6 hours) - Preparing overview of Challenge to share with partners (4 hours)	Potential costs to be incurred re making relevant data assets available
April-May 2023	Industry participant confirmation	- CoLC to lead with support from CoLPA: - Preparing list of potential industry participants and preparing documentation to provide an overview of the Challenge, its objectives and the commitment required (8 hours) - Making approaches to industry partners and attending meetings with them (8 hours) - Finalising industry participants (4 hours)	N/A
April-May 2023	Technology participant applications	- CoLC to lead with support from CoLPA: - Agreeing eligibility/assessment criteria for applications (6 hours) - Drafting call for application, application form and publicising across CoLC/CoLP channels and partner networks (10 hours) - Recruiting partners to review and assess applications (4 hours) - Review and assessment of applications (10 hours) - Meetings to discuss application review including compiling comments and finalising list of successful applicants (10 hours) - Informing applicants of outcoming and providing feedback to applicants where requested (6 hours)	N/A
May 2023	Challenge finalisation	- CoLC to lead with support from CoLPA: - Reviewing and finalising Challenge schedule and features (6 hours) - Meetings to finalise Challenge including meetings with all participants for gathering feedback (10 hours) - Circulating final Challenge schedule to all participants and scheduling all sessions across relevant diaries (12 hours)	N/A
June-July 2023	Challenge delivery (based on a 10-week sprint)	- Ensuring CoLC or CoLP representation at each Challenge session to act as facilitator and action any feedback or follow-up (50 hours) - CoLC to lead on regular check-ins with participants to gather feedback (10 hours)	N/A

		- Also providing any additional scheduling or other support to participants and partners during Challenge (20 hours)	
September2023	Public showcase event	- CoLC to lead with support from CoLPA/CoLP: - Confirming format and participants for the event, including briefing sessions for any panel members and/or other presenters (8 hours) - Creation of any video asset/content to support event (10 hours) - Compiling invitee list, sending out invitations and confirming attendees (6 hours) - CoLP and CoLPA attending event and follow-up (4 hours)	£10,000[2]
October 2023	Challenge evaluation conducted and published	- CoLC to lead with support from CoLPA: - To gather any data required for evaluation purposes eg entry/exit surveys, additional feedback sessions from partners and participants (10 hours) - To review and analyse feedback gathered and prepare draft report (10 hours) - External support on report design and finalisation (6 hours) - Finalising and publishing report (4 hours)	£10,000

[2] This represents total estimated cost to be covered by CoLC

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank

Document is Restricted

This page is intentionally left blank