

Committee: Economic and Cyber Crime Committee – For information	Dated: 06/09/2021
Subject: National Lead Force Update	Public
Which outcomes in the City Corporation’s Corporate Plan does this proposal aim to impact directly?	1,10, 12
Does this proposal require extra revenue and/or capital spending?	N
If so, how much?	NA
What is the source of Funding?	NA
Has this Funding Source been agreed with the Chamberlain’s Department?	NA
Report of: Assistant Commissioner McLaren	For Information
Report author: Alix Newbold	

SUMMARY

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

- Action Fraud virtual assistant freeing up time equivalent to 3 FTE
- Next Generation Service invitation to tender launched on 1 July
- Semi-automation of banking alerts increasing the likelihood of repatriation of losses
- Robotic data transfer increasing the speed of victim referrals from Action Fraud to the Economic Crime Victim Care Unit
- A national ghost broking week of action resulting in 7 arrests and 78 social media account disruptions

Recommendation(s)

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

MAIN REPORT

BACKGROUND

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

CURRENT POSITION

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

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

Action Fraud virtual assistant frees up time equivalent to 4 FTE

3. The chatbot virtual assistant service continues to deliver improvements to the online user experience. Since its roll out in April the web chat abandonment rate has been reduced by 86% and the virtual assistant is managing demand equivalent to 4 full time web chat advisors. In June alone, almost 22,000 website visitors accepted this service.
4. In June, improved call routing (IVR) went live, guiding victims to appropriate links or information, and making it easier for them to report via the web tool. As a result, live cyber call volumes saw a significant reduction as the IVR helped redirect calls more efficiently. This led to improvements in both the speed of answer and the call handling times required to support the victims of this crime type.

Next Generation Service invitation to tender launched on 1 July

5. Following Home Office and Treasury approval the invitation to tender to tender for the Next Generation Fraud and Cyber Reporting & Analysis Service was launched on July 1. To date over 100 bidders have expressed an interest in participating. There will be a number of key milestones to follow, including the closure of the new bidders process at the end of August. The current provider, IBM, has agreed a short extension of the contract to ensure there is no disruption to service until the new system is ready to go live. We continue to engage with policing and the wider counter fraud community throughout the process.

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

6. COLP is responsible for providing first contact support for victims who report to Action Fraud. It is also responsible for developing and disseminating national protect messaging for policing based upon latest crime reporting trends. COLP is constantly looking for new channels to strengthen the reach and impact of fraud prevention advice to the public.

Semi-automation of banking alerts increases the likelihood of repatriation of losses

7. Identifying reports to Action Fraud where money had very recently been paid to a fraudster (funds at risk) and alerting the recipient bank has proven incredibly successful for NFIB. It has sent 10,382 alerts relating to £208m funds at risk

which has resulted in a minimum of £6.5m repatriated back to victims since July 2017.

8. This manual process has now been replaced through a technological solution. This solution identifies reports meeting the relevant criteria and either generates and sends an alert via email (30% of total), or creates a work process for review by NFIB staff to determine if an alert should be sent. This has reduced the manual review of reports by 30% and has reduced the time from report received to alert dissemination from approximately 3 days to 1 day. This will be further reduced to 2 hours once a residual licence issue is resolved. This will provide recipient banks with more opportunities to intervene in fraudulent transactions and take action to return funds to victims where possible.

Robotic data transfer increases the speed of victim referrals from Action Fraud to the Economic Crime Victim Care Unit

9. Sections of the process of extracting, formatting and transferring data from the current AF/NFIB system into the ECVCU system are now automated resulting in time savings for Victim Care Reviewers who would have ordinarily completed this manual process. The process is now run weekly, instead of monthly, meaning quicker data access for ECVCU, a shorter report to referral time for victims which could have been as long as 60 days, but will now take no longer than 14 days. The new process has reduced the administration needed to prepare and send the data, resulting in a saving of at least 20 hours per month processing time for staff which can be used to support more victims.

Ticketing fraud prevention campaign

10. The Action Fraud ticket fraud campaign in June achieved 16m impressions (number of timeline deliveries) and 6m reach (number of unique users who have seen the content). Messaging was developed with UK Finance and Star (the Society of Ticket Agents and Retailers). Social media material, including digital graphics were circulated to forces and via the Multi Agency Campaign Group. Bespoke assets and messaging for Euro 2020 were also developed featuring official UEFA advice reminding the public that third party ticketing sites and secondary ticketing platforms are not authorised to sell tickets to games.

Anti-phishing prevention campaign

11. The annual #MulletOver anti-phishing campaign in June raised awareness of how to spot phishing messages and where to report them. Social media containing messaging and assets were developed and circulated to forces and via the Multi Agency Campaign Group. The campaign achieved 25.8m impressions (number of timeline deliveries) and 9.8m reach (number of unique users who have seen the content).

Holiday fraud prevention campaign

12. The campaign in May achieved 16.4m impressions (number of timeline deliveries) and 7.1m reach (number of unique users who have seen the content). The messaging was developed with ABTA and aims to help people to spot the

signs of holiday fraud before booking holidays online. Press release, social media schedule and campaign assets were developed and distributed to partners and forces.

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

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

Project Otello

14. City of London Police has agreed tactical and operational plans for the sustained improvement to the policing response towards Courier Fraud and Romance Fraud under Project Otello. The aims of the extended work programme are to:
 - a. impact positively on levels of organised criminal activity and bring offenders to justice;
 - b. provide disruption opportunities where investigation is not viable;
 - c. identify and support victims at the earliest possible stage, even where reporting has not taken place; and
 - d. increase levels of intelligence to facilitate better proactive opportunities.
15. To that end we have identified Single Points of Contact / “Bronze” officers in every force who will support the joint delivery of Project Otello against COLP’s 4P plan. A webinar in July 2021 was attended by all Bronze officers.

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

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

Operation Ironclad

17. The City of London Police’s Insurance Fraud Enforcement Department (IFED) conducted a ‘week of action’ at the end of June as part of a crackdown on ghost broking across the country. Individuals or groups, known as ‘ghost brokers’, pose as intermediaries for well-known insurance companies, claiming they can offer legitimate car insurance at a significantly cheaper price. It is typically carried out in one of three ways:

- a. they will either forge insurance documents
 - b. falsify someone's details to bring the price down, or
 - c. take out a genuine policy, before cancelling it soon after.
18. The insurance industry identifies ghost broking as one of the key threats at this time. Industry reported a significant volume of ghost broking activity (via Insurance Fraud Bureau (IFB)) Investigations submissions. In 2020, 38% of all requests featured ghost broking. IFED received a 59% rise in ghost broking referrals in 2020 in comparison with 2019.
 19. The monetary value of these frauds range from the low thousands to hundreds of thousands, depending on how long and to what scale the broker has been operating. Several cases have clear links with other criminality, including county lines. Perpetrators frequently target vulnerable victims within their own communities and exploit people who do not speak English.
 20. With ghost broking, the victim is at risk of driving illegally with no insurance, incurring a fine for failing to have valid insurance, receiving 6 points on their driving licence, having their vehicle seized and a fee required for release (or the vehicle being crushed), and further loss of money as the victim has to pay for a further legitimate insurance policy and/or is unable to make a claim. Most victims have no idea they are uninsured until they are stopped by the police or try to make a claim on their insurance.
 21. Officers were deployed across eleven operations in London, Essex, West Yorkshire, Bristol, West Midlands, Derbyshire and Wales. IFED also employed alternative methods of disposal - such as cease and desist notices and online disruption. The week saw the following results:
 - 10 warrants executed
 - 7 people arrested
 - 14 searches
 - 5 cease and desist notices served
 - Over 100 pieces of evidence seized
 - 78 social media accounts put forward for removal (working with Facebook and Instagram)
 22. Media engagement was a key part of the protect strategy. An article in the Saturday Times print and online editions showed a warrant and arrest in South London and featured an interview with IFED and its work to remove fraudulent profiles from social media. Targeted Instagram messaging reached 12,146 people reached (90% from promotion, 10% organic).

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

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

Economic Crime Academy

24. The Academy has been working with Coventry University and the Cabinet Office to produce a third e -Learning course called 'Fraud Risk Assessment', which sits on the Future Learn platform. This course will be delivered across government departments as part of their counter fraud strategy.
25. A new course called Demystifying Blockchain and Cryptocurrencies has finished its pilot and will now be rolled out to all who wish to undertake it within the City of London Police and will be available to other law enforcement agencies (UK and Overseas) for use on a commercial basis. A new cyber course, called Cyber Enabled Fraud, has been commissioned by the Academy and this will cover several different cyber fraud typologies used by criminals, with a view to improving awareness and knowledge in this growth area of fraud.

Nationally Networked Proactive Economic Crime Teams Pilot

26. Terms of reference and performance frameworks have been agreed for the pilot across four ROCUs. Tasking and coordination processes are being tested with all ROCUs to ensure future proofing for any further investment. All ROCUs have commenced recruitment with open events, discovery days and workshops to encourage applications. ERSOU has identified 4 of their posts and a release date of October is planned.

CONCLUSION

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