AGENDA ITEM 8a

Strategic Policing and Crime Board

19 February 2019

Police and Crime Plan Priority: *Reducing Crime and Harm*

Title: *Fraud*

Presented by: *Jenny Birch/ ACC Southern*

Purpose of paper

1. The purpose of this paper is to describe West Midlands Police's (WMP) approach to the growing threat of fraud in line with the Police and Crime Plan priority, 'Protecting from Harm', specifically reducing the number of victims and ensuring a holistic prevent, prepare, pursue, protect (4P) approach is taken. This paper is for discussion.
2. This paper will explain the development and performance of WMP's Economic Crime Unit (ECU), the 4P approach[1] taken to the investigation of fraud and cybercrime, partnership working and the key challenges facing the force.

Background

3. Following a governmental review of fraud in 2006, it was concluded that fraud was a significantly under-reported crime and, while various agencies and forces were attempting to tackle the issue in isolation, a joined up approach was needed to reporting, recording and analysing fraud.
4. The review resulted in the creation of a national single point of reporting for fraud, ActionFraud, and the National Fraud Intelligence Bureau (NFIB) as part of the lead force for fraud, the City of London Police.
5. All reports of fraud and cybercrime are now reported centrally via ActionFraud. This can be done via phone or via an online reporting tool on the ActionFraud website.

[1] Prevent, prepare, pursue, protect

6. ActionFraud works alongside the NFIB to ensure any reports are linked and enhanced with other data when available and then assess whether reports have any lines of enquiry.

7. If any lines of enquiry are identified, the reports are disseminated to the most appropriate agency to deal with, which includes the police, Department of Work and Pensions (DWP), National Crime Agency (NCA) etc. Typically reports are disseminated to geographical police forces based on where any identified offender resides.

8. It is then for the individual force or organisation to assess the reports and decide if they represent viable investigations.

9. When a report is received, West Midlands Police Crime Services Team (CST) will, at the direction of the ECU, create a fraud "non-crime" number that is recorded on the WMP IT systems to ensure that there is a record of the offence(s) and the progress of the investigation can be captured locally.

10. If the fraud or cybercrime offence is reported to police directly either via 999 or 101, Force Contact make an assessment as to whether the incident is a "call for service", i.e. it is a crime in action or if there is a vulnerable victim involved.

11. If the incident is a call for service, an officer is dispatched, a primary investigation is commenced and a non-crime number taken out (as crimes can only be recorded by Action Fraud). If the incident is not a call for service, the caller is sign posted to ActionFraud to report the matter.

12. A summary of the process described in paragraphs 10 to 12 can be found at Appendix A.

Introduction

13. WMP ECU comprises of five teams, each with a distinct remit:

    a. **Financial Investigation Team** - Conduct financial investigation using the powers conferred under the Proceeds of Crime Act (2002).

    b. **Investigation Management Team** (IMT) - Receive, assess and allocate for investigation, where appropriate, the referrals into WMP from ActionFraud.

    c. **Complex Fraud Investigation Team** - Conduct investigations into serious and complex fraud offences. This team is also responsible for the coordination of WMP's response to the electoral process and the investigation of reports of electoral fraud.

    d. **Cyber and Fraud Investigation Team** - Conduct investigations into complex cyber-enabled[2] fraud and cyber-dependent[3] crime.

[2] Defined as "traditional" crimes, which can be increased in scale by use of information communications technology. For example, where a criminal uses account log in details stolen from a member of the public to transfer money in and out of their account without authorisation.

e. **Proactive Investigation Team** - Assess and investigate Suspicious Activity Reports (SARs) that are submitted by businesses within the financial regulated sector. Also conduct proactive investigations into key nominals or groups involved in serious and organised crime.

ECU Development and Performance

14. The unit has developed in the last 12 months towards a more focussed approach on the investigation of serious and organised economic and financial crime, and the provision of support to such investigations carried out by other WMP teams and partners such as DWP and Her Majesty's Revenue and Customs (HMRC).

15. The unit are currently involved in 16 investigations linked to organised crime groups, which has increased from six recorded in May 2018. Unfortunately no figures exist prior to January 2018 to offer a comparison.

16. WMP currently have 6 active organised crime groups that are involved in fraud and economic crime such as money laundering. This equates to 7% of the total number of active groups recorded for the Force. Two of these groups were mapped by the ECU over the last year.

17. The team, in conjunction with the Regional Cybercrime Unit, are also continuing to develop the cyber-dependent investigative capability described in 14(d) above, in line with the requirements of the National Cybercrime Programme.This includes five resources from the West Midlands, funded by the ECU.

18. There is a nationally agreed performance framework for this capability, as below:

    a. 100% of ActionFraud referrals will be investigated (PURSUE[4])

    b. 100% of victims who report to ActionFraud will get advice in person or over the telephone to prevent them becoming repeat victims (PREPARE[5]/PROTECT[6])

    c. 75% of organisations and the public who receive PROTECT advice will change their behaviours as a result

    d. 75% of organisations who receive PREPARE advice will develop or review incident response plans and test them

    e. 100% of young people identified as vulnerable to cybercrime will get PREVENT contact and intervention from a PREVENT[7] officer where appropriate.

19. The WMP cyber-dependent capability went live as of 30 April 2018. To date, the team have received 28 cyber-dependent reports of differing types such as

[3] Defined as crimes where a digital system is targeted by means of a criminal attack. For example, the use of a specially designed code to hack into a victim's computer to steal sensitive personal information such as account log in details and passwords.
[4] Defined as activity taken to investigate, prosecute and disrupt offenders
[5] Defined as activity designed to assist in the preparation for when crime occurs and to mitigate the impact
[6] Defined as activity relating to victims
[7] Defined as activity relating to offenders

sextortion[8] (6), hacking (12), denial of service attacks[9] (2) and general cyber-attacks (8).

20. All of these reports have had a proportionate investigation conducted and all of the victims have received appropriate crime prevention (PROTECT) advice. As yet, the performance measures regarding behaviour have not been measured due to the complexity of assessing the changes in behaviour resulting from the advice provided.

21. Offenders have been identified in 43% of these cases and none meet the criteria laid out in the performance measure described at 18 (e).

22. Whilst there are currently no national or force defined performance measures in place to assess the ECU, a national fraud strategy workshop is taking place in February 2019 to discuss the national strategy and corresponding performance framework. The ECU are also working on the development of a local strategy to dovetail into this wider strategy.

23. NFIB report on the national and local force performance bi-annually. The dashboard reports in relation to WMP for fraud and cyber-dependent crime recorded between April and September 2018 can be found at Appendix B and C respectively.

24. The key fraud findings for this period are:

    a. The total number of recorded crimes[10] has increased by 17% to 17,185 compared with the previous six month period. This is in line with national trends.

    b. Victim losses have dramatically increased by 85% to £33.3 million.

    c. Businesses continue to represent the highest proportion of victims of fraud as opposed to individuals. This has been a consistent picture over the last two years.

    d. The most common type of fraud by volume is cheque, plastic card and online fraud and by loss is fraud by abuse of position of trust[11]. This has been a consistent picture over the last two years.

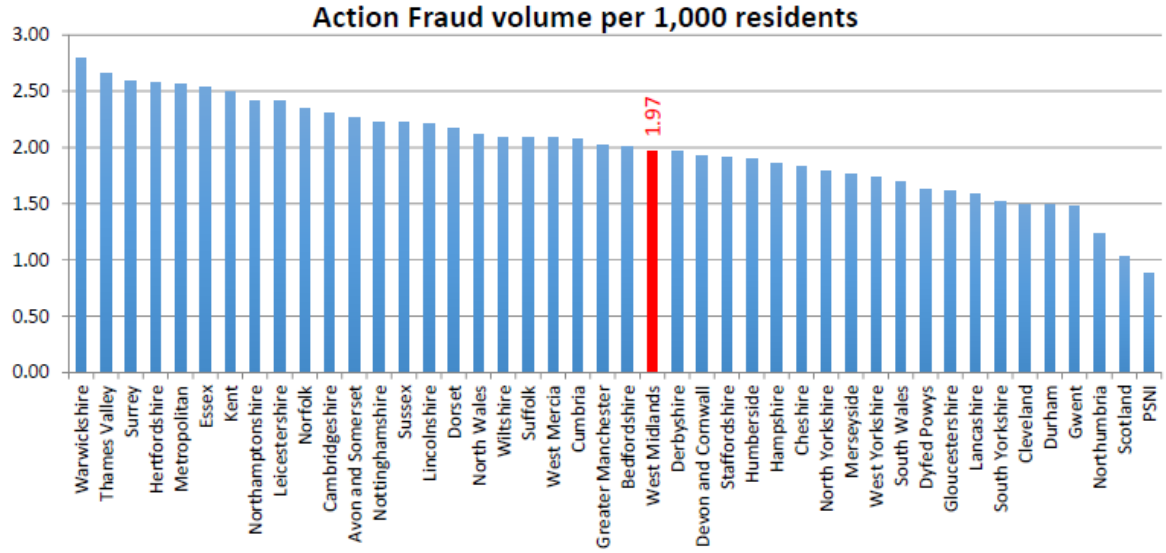
25. During the period there have been 821 outcomes recorded, 52 of which were positive; 32 resulted in charge, 13 in caution and seven in a community resolution. A further 24 were referred to another investigative agency. Of the remainder, a number have been filed as no further action or remain as part of an ongoing investigation. No suspect was identified in 268 of the reported cases.

[8] Defined as the practice of employing non-physical forms of coercion to extort money or sexual favours from someone by threatening to reveal evidence of their sexual activity.
[9] Defined as a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet
[10] As reported to ActionFraud, Cifas (who hold the National Fraud Database, which allows organisations to share data on thousands of fraud risk cases) and UK Finance (who represent more than 250 firms across the banking and financial industry)
[11] 'Abuse of position of trust' involves those individuals who are empowered/trusted to protect money and then de-fraud victims via this process.

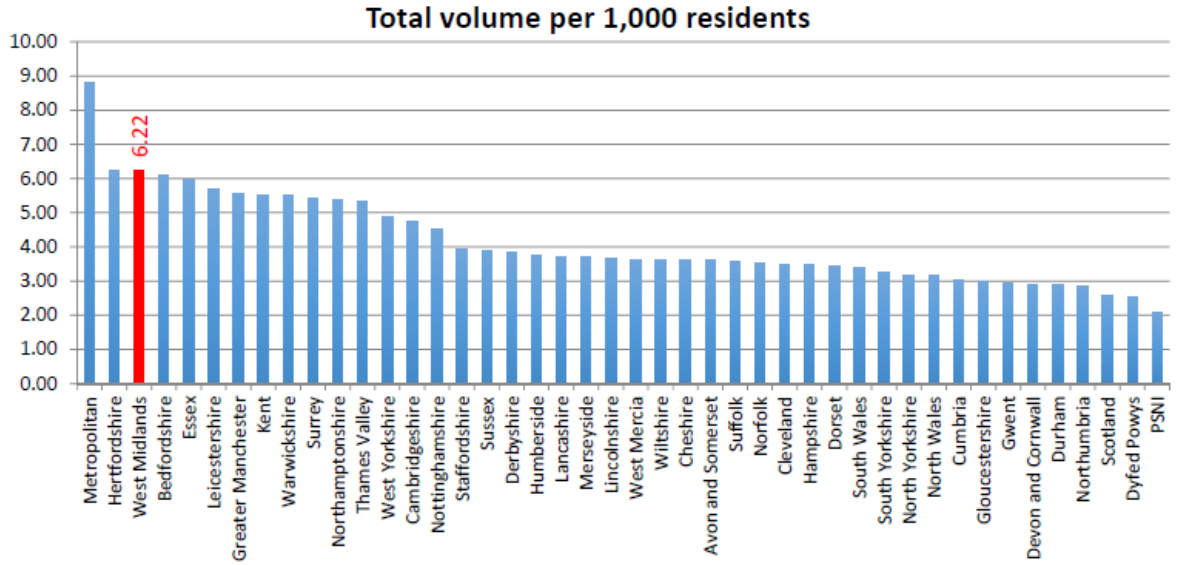
26. In previous reporting periods, the number of judicial outcomes has averaged 5% of the number of crime referrals received. For the April to September period, WMP have achieved a 3% outcome rate. This reduction is likely to be as a result of the length of time it taskes to investigate fraud given the complexity of the criminality involved and the increased use of encryption and other technologies to enable offending. The global nature of fraud offending, with offenders often living abroad, can also impede the progress of investigative work. Work is ongoing by the department to explore the reasons for this reduction in more depth.

27. The latest NFIB profile also indicated that 84% of fraud reported nationally is cyber enabled. For WMP, the most common enabler is the mobile phone, followed by online sales and the use of a false identity. Phones have been the most common enabler for WMP for the last two years averaging 32% of all fraud reports.

28. The graph below compares the volume of ActionFraud reports for the West Midlands to other areas across the country.



29. However, when all reports of fraud are considered, including those made to Cifas and UK Finance, WMP rate far higher i.e. have had a greater proportion of frauds reported as per the graph below. It is likely that this due to the fact that Birmingham hosts the headquarters of many major banking institutions, such as Royal Bank of Scotland (RBS) and HSBC.



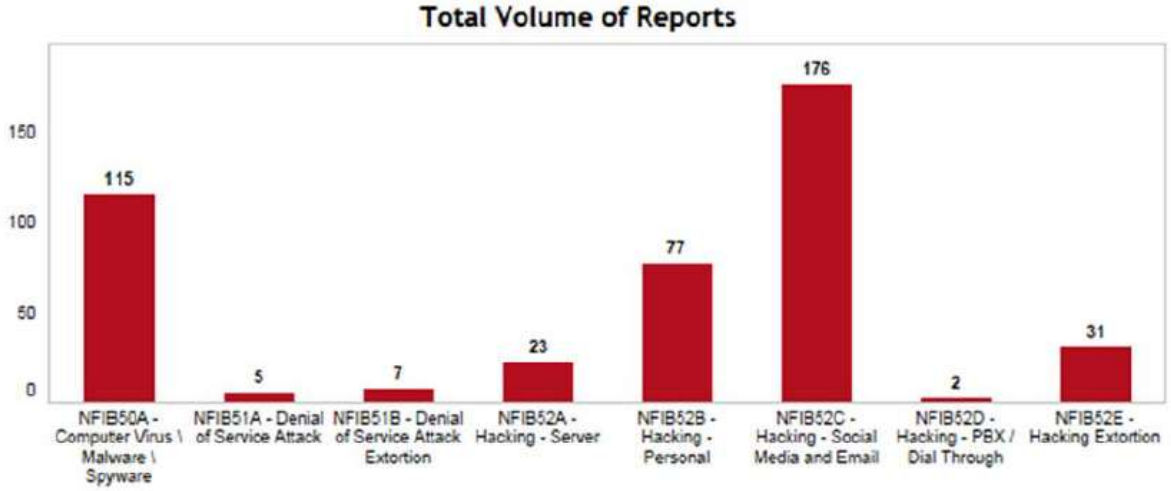
30. The key cyber-dependent findings for this period are:

    a. Hacking represented the highest proportion of offences (176) during the six month period with estimated losses totally £328,000. This is followed by Malware/Spyware.

    b. Victim losses have dramatically increased by 85% to £33.3 million.

    c. Conversely to the fraud profile, the highest proportion of victims of cyber-dependent crime are individuals.

31. The graph below shows the types of cyber-dependent crime offences recorded during this period. This has remained fairly consistent over the last 18 months.



Intelligence Analysis

32. In addition to the bi-annual profiles produced by NFIB and referenced above, NFIB publish monthly Victim Information Reports. These reports provide sanitised victim records for all reported fraud within that month that includes information regarding

the postcode where that victim resides, the fraud category and the victim's self-described ethnicity, their age and their financial loss.

33. Unfortunately there is no further granular information available to the ECU that might assist with a more detailed analysis of the demographics of fraud victims other than in broadly general terms.

34. Analysis of WMP held records of fraud non-crimes does not consistently provide any more specific victim information due to the way that the ActionFraud disseminations are received and recorded by the Force. This is important as detailed demographic analysis would enable the force to target protective and preventative strategies.

35. As referenced previously, disseminations to local forces are typically based on the home address of any identified offender. As fraud offenders tend to commit offences against numerous victims, one dissemination from NFIB can actually relate to multiple victims across multiple locations/countries. For example, one live investigation that originated from one NFIB dissemination relates to upwards of 30 victims.

36. However, the information provided by NFIB and that which can be obtained from WMP systems does provide the opportunity for some limited analysis.

37. A strategic analysis of fraud has been commissioned via the Strategic Intelligence Team with an expected completion date of March 2019.

38. A more tactical monthly analysis product has also been commissioned via the Tactical Intelligence Team, the outcome of which is expected imminently.

39. The ECU has an intelligence analyst post within its build, which is currently vacant. A recruitment process is in progress and it is anticipated that the post will be filled in April 2019. The responsibility for completion of the monthly product will then fall to the new post holder.

Lessons Learned

40. In the last 12 months, the ECU has been part of a thematic inspection around fraud completed by Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS). A thematic inspection will not reference a specific force's performance but will provide overall findings that apply to all Forces subject to that inspection. The final report has not yet been published.

41. In addition to the above inspection, the ECU were subject of a voluntary peer review conducted by the National Police Coordinator's Office, part of City of London Police.

42. On the basis of the feedback from both of these processes, a 4P delivery plan was developed to address the identified areas for development. This plan is a living document where progress is reviewed monthly within the ECU and the results are

fed into the wider Force CID Delivery Plan, monitored via a monthly departmental Strategic Delivery Board.

43. The following section describes the key developments made within the ECU to improve the systems and processes to address the highlighted areas.

PURSUE

44. The initial assessment of fraud referrals has been transformed to incorporate use of the nationally recognised Measurement of Risk in Law Enforcement (MoRiLE) risk assessment methodology. This tool allows the assessor to consider the impact of the offence under assessment on the victim, the community and the environment. In addition, the assessor considers the credibility of the threat, scale of the criminality involved and any identified victim vulnerability.

45. The tool then provides a score based on the answers provided. Based on the results analysis of a trial period of use of this tool, the ECU were able to determine the scoring levels that now define low, medium and high risk fraud reports.

46. In order to complete the assessment tool effectively, the IMT complete a thorough initial investigation into the complaint using a wide range of intelligence and information in order to determine its viability for allocation to an investigative team.

47. The tool has been used to make the initial assessment of all of the referrals received since April 2018. This has resulted in an estimated 10% uplift in the number of fraud referrals that are now allocated for disruption or investigation.

48. To accompany this change to the initial assessment, the historic investigative strategy has been revised. The new strategy sets out the recommended pursue or preventative activity that should be carried out dependent on the identified risk level.

49. It is recognised that WMP do not have sufficient resource to investigate every reported fraud offence, however, this strategy makes it clear that no activity in response to a received report is not an option.

50. For example, if a report has been assessed as low risk, the IMT consider different disruption tactics in relation to the offender such as sending cease and desist letters warning them that their conduct will not be tolerated, close down bogus websites, physical visits to offenders and arrests for other offences for which they may be wanted.

PROTECT

51. Both fraud and cybercrime can have a big impact on the health and wellbeing of victims, both personally and financially.

52. The latest NFIB fraud profile identified that 4 out of 20 victims identified themselves as vulnerable with a higher proportion (33%) of victims declaring the impact of the

crime was “significant” than the national average. 7% of victims reported the impact as “severe”.

53. The latest NFIB produced cyber-dependent profile identified that 5 out of 20 victims identified themselves as vulnerable with a higher proportion of victims declared the impact of the crime was “severe” than the national average (8.3% compared with 6.2%).

54. The National Economic Crime Victim Care Unit (NECVCU) commenced in 2017 and is funded by the Home Office. The team were set up to identify vulnerable victims of fraud and offer a service to protect them and prevent them becoming repeatedly targeted. The victims who are part of this project will not have been disseminated to forces for further investigation of their crimes, therefore will not have received any direct contact (other than an e-mail or letter detailing the status of their report).

55. The NECVCU provide a three-tiered model of support based on an initial assessment of vulnerability within particular types of victims. The three levels of support are defined as:

    a. **Level 1** – less complex case whose victims will be provided with initial management and appropriate support with contact made to signpost services or to provide advice tailored to the victim.

    b. **Level 2** – more complex cases whose victims will be contacted by a specialist team for a detailed needs and vulnerability assessment and advice will be tailored to their individual needs.

    c. **Level 3** – require a home visit to provide local level support focused on safeguarding and supporting the most vulnerable at-risk individuals using a multi-agency approach or to manage other issues identified through level 2 contact.

    As part of the agreement between WMP and the NECVCU, level 1 victims are contacted by telephone to offer basic advice and support. Level 2 victims are dealt with by advocates in City of London Police.

56. WMP are one of two pilot forces trialling the concept of a local ECVCU. The role of the ECVCU is to provide support to those victims of fraud and cybercrime who are assessed at level 3. The team comprise of two Detective Constables (DCs) allocated from the main ECU establishment and overseen by the Detective Sergeant overseeing the Cyber and Fraud Investigation Team.

57. In addition to the level 3 referrals allocated to WMP from the NECVCU, the other teams within the ECU and the wider Force have the ability to request assistance from these officers where they have identified a victim that would benefit from extra support either due to the psychological impact of the crime they have suffered and/or if they are identified as a vulnerable victim.

58. For example, the ECU Proactive Investigation Team regularly identify potential vulnerable victims from their review and assessment of the SARs the Force receives. These victims are referred into the ECVCU team.

59. The ECVCU team offer a wide range of supporting activities including:

    a. An advocacy service for the referred victims with financial institutions

    b. Referral service to partners to further support the victims eg. Mental Health Services, Social Services, Age Concern UK etc

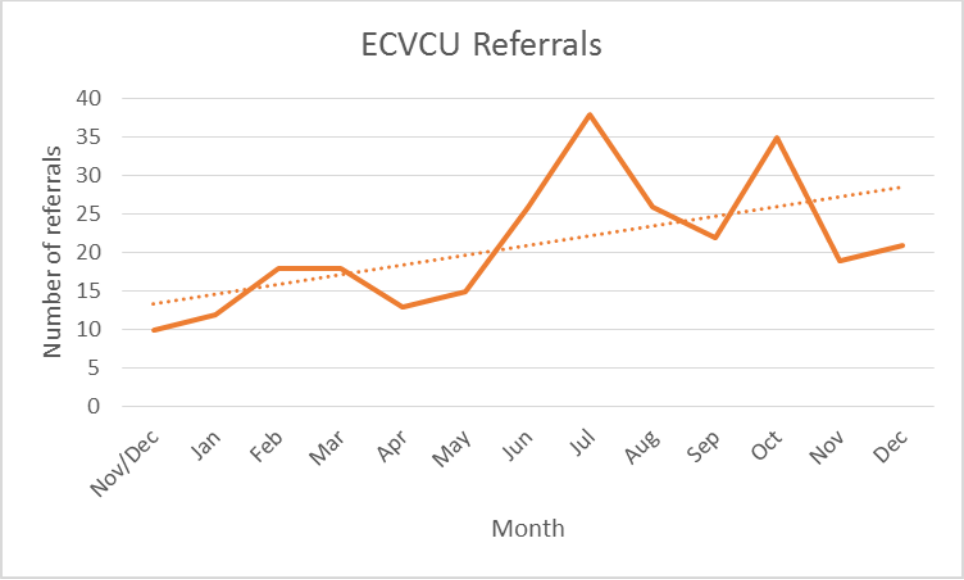
    c. Onward referral for more long term victim support to partners such as Victim Support

    d. Liaison with ActionFraud and NFIB to discuss the progress of their case and to explain the crime recording and investigative process

    e. Provision of bespoke financial advice and online security measures to help to prevent the victms from becoming repeat victims in the future

    f. Installation of telephone blocker technology from TrueCall. This blocks 95%+ of all nuisance calls and reduces the ability of offenders to contact fraud victims over the telephone. This technology was funded from the WMP asset recovery fund, funded by the assets recovered under the Proceeds of Crime Act.

60. The team commenced receiving referrals in November 2017. The graph below shows the number of referrals per month dealt with by the team:



61. Whilst there is an upward trend in the number of referrals the team have received, due to the team's limited capacity, the ECU have not been in a position to widely publicise this facility in a systematic way.

62. In order to increase capacity within the team to support victims of fraud and cybercrime, the ECU have participated in a Force level volunteer recruitment process under the Citizens in Policing. We are in the process of recruiting 16 volunteers from the communities of the West Midlands.

63. The ECU are working with the Victim Support charity in order to ensure that these volunteers are appropriately trained and are working in a supportive and learning environment. This will not only enhance the service that Victim Support are able to provide to victims of fraud and cybercrime but also increase the scope for investigators to refer their victims for specialist support.

64. The ECU identified the need for a Protect Coordinator to assist in setting the protect strategy for the ECU and wider Force, coordinate the activity of the ECVCU, partnership working and to coordinate the continued development and delivery of protect messaging to colleagues and partners.

65. A further DC was identified from the main ECU establishment to fulfil this role on a short term basis. The initial protect strategy has now been developed.

66. The Protect Coordinator, in conjunction with the Force's digital Police and Community Support Officer (PCSO), have obtained the agreement to mobilise 16 Neighbourhood Policing Unit PCSOs to act as a network of fraud/cyber SPOCs who will deliver protect messaging directly to the communities of West Midlands Police.

67. The training inputs for these PCSOs are currently ongoing and it is anticipated the the network will be fully formed from April 2019.

68. The role became vacant as of 14 January 2019. However, it is the ambition of the unit to create a newly established police staff post to fulfil this role. The post has been evaluated and is going through Force processes towards recruitment. The post is part funded by a Police Transformation bid submitted via the National Cybercrime Programme.

PREVENT

69. There is an ambition to move towards working more within the Prevent agenda to deter and divert (potential) fraud and cybercrime offenders. This is included in the ECU 4P delivery plan and will be developed in the forthcoming twelve months.

70. The use of Serious Crime Prevention Orders in relation to fraud offenders is rare for WMP. However, the orders can be very beneficial in deterring repeat offending and the unit is looking to explore this as an option moving forward in the next 12 months.

PREPARE

71. In addition to the intelligence work described, the ECU 4P delivery plan addresses a number of areas that will assist in the preparedness of the unit and the Force to address the threat from fraud and cybercrime:

    a. The exploration of new partnership data sharing opportunities working with the Partnership Intelligence Liaison Team within the Force Intelligence department

b. Creation of strategy and practical guidance around the investigation of such offences including protect advice

Some progress has been made in both of these areas.

72. The ECU now share a memorandum of understanding with HMRC and the Royal Mail Group. However, there is further work to be done in terms of a long term sustainable and mutually beneficial information sharing agreement.

73. The ECU intranet site is in the process of being updated with the latest strategy and guidance as is the external facing WMP internet site. However there is more work to be done in this area.

Partnership Working

74. The ECU are involved with various partners across the West Midlands in order to share expertise and best practice between all of those affected by fraud and cybercrime.

75. The main partner is obviously ActionFraud and NFIB. The ECU are in constant communication with these teams ensuring that our proceses and understanding continue to evolve based on national best practice. WMP also engages with ActionFraud in relation to their national communications campaigns.

76. The next such campaign is the “Secure your new device” to be run this month. This aim is to alert the public to the simple and practical steps they can take to secure the new computer, laptop or smartphone they’ve bought, or received as a present, over the holiday period.

77. According to a 2017 consumer survey by PriceWaterhouseCoopers, 50% of consumers said most of their spending on Black Friday will be on electricals and technology. The campaign will be supported by Regional Organised Crime Units, police forces, ActionFraud, as well as multi-agency partners.

78. The Detective Inspector in charge of the ECU is a key member of the Midland Fraud Forum. The aim of the forum is to promote awareness of fraud issues and best practice in countering fraud in order to educate everyone on effective fraud prevention measures. The group are aware that fraud occurs in both private and public sectors and will continue to escalate until a joined up partnership approach is adopted. Other members of the forum include other investigative agencies such as the Insolvency Service and the Insurance Fraud Bureau as well as businesses such as EY, formerly Ernst Young, and Pinsent Masons.

79. During the last 12 months, the ECU have been engaged in joint operations with the Insurance Fraud Bureau, HMRC, DWP and the Royal Mail Group. The latter partnership has resulted in five arrests, three charges and two convictions for postal fraud related offences.

80. The ECU are also working with NHS Fraud in relation to fraud within the health service. This is a relatively new relationship that will continue to develop over the forthcoming months.

81. The ECU are the lead for the implementation and monitoring of the nationally advocated banking protocol, which involves partnership working with Trading Standards. The protocol is an initiative between the police, banking institutions and Trading Standards. Its aim is, at the earliest opportunity, to identify vulnerable victims who are in the process of being defrauded of funds from their bank accounts by unscrupulous criminals and to intervene to prevent these crimes.

82. Vulnerable victims identified via the banking protocol are referred into the ECVCU for ongoing support and advice.

83. The table below shows the results of this initiative since its inception in September 2017:

Month	Incident Logs	Arrests	Loss Prevented
Sep-17	15	0	£27,250
Oct-17	27	1	£56,000
Nov-17	28	1	£62,810
Dec-17	24	1	£69,970
Jan-18	18	0	£51,623
Feb-18	22	1	£85,030
Mar-18	32	0	£108,000
Apr-18	23	1	£43,997
May-18	42	4	£155,088
Jun-18	40	0	£27,840
Jul-18	42	0	£134,869
Aug-18	41	0	£57,030
Sep-18	47	1	£78,480
Oct-18	40	0	£98,093
Nov-18	31	1	£78,942
TOTALS	**472**	**11**	**£1,135,022**

84. The team also provide continuous professional development inputs to our partners such as the Crown Prosecution Service, RBS, the Coventry Building Society, the Dogs Trust charity to share our understanding of fraud and cybercrime as well as providing protect advice. This is in addition to the WMP internal training and development that the ECU deliver year on year for the Force.

85. The unit are currently working in partnership with Birmingham City University providing placements for two law students within the team in order to gain experience of working within a law enforcement environment and dealing with real life reports of complex crime. The placements began in October 2018 and are due

to be completed in May 2019. An evaluation of the value of the placement both to the students and the ECU will be undertaken in June.

Key Challenges and Future Opportunities

86. The main key challenge facing WMP at the current time is the volume of fraud and cybercrime reports made and disseminated to the force versus the available resource to investigate.

87. Whilst the national and local initial assessment and investigation processes go some way to manage the demand, this is not sufficient as numbers of reported crimes continue to grow.

88. However, the new Serious and Organised Crime Strategy has pledged to increase the frontline capacity and capability to tackle fraud. In support of this, the creation of a regional Fraud Coordinator post has been proposed. This will deliver a more coordinated approach to fraud investigation across the region especially in the area of protect/prevent.

89. The increased sophistication of fraud and cybercrime perpetrators represents challenges to the police. Typically we do not have the tools or expertise within the force to move at pace with increased use of technologies to enable this type of offending.

90. The advent of the National Economic Crime Coordination Centre, a part of the NCA that commenced in October 2018, may alleviate some of issues as it is provides a multi-agency centre that has been established to deliver a step change in the response to tackling Economic Crime. However, we are yet to understand any additional demand this may generate at a local level.

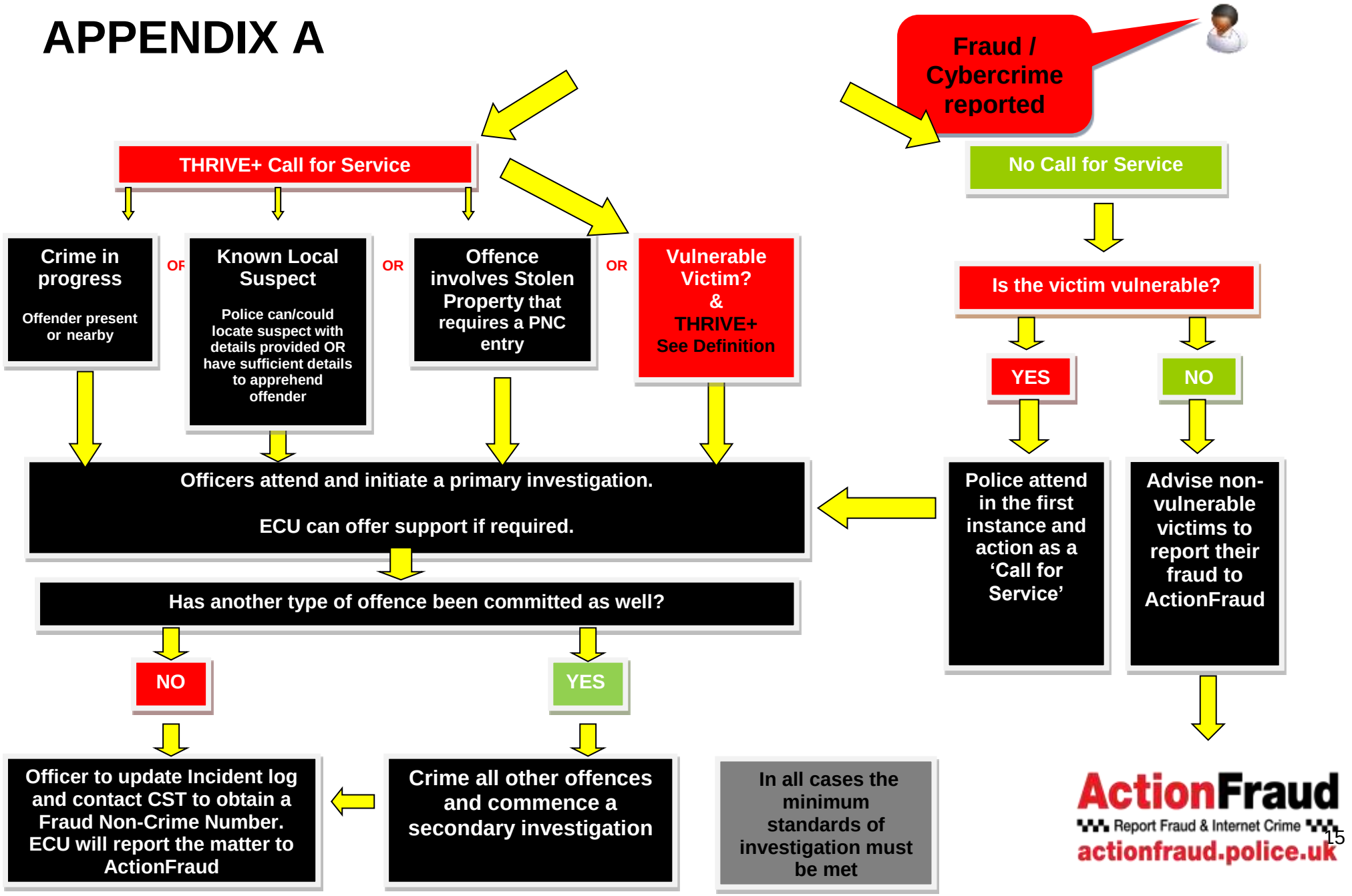
91. WMP ECU has been invited to feed into the formulation of the national fraud strategy being drafted by the City of London Police. A workshop including regional partners has been arranged for 28 February 2019. This will provide a good opportunity to influence national policy and to share the developments the unit has delivered and the challenges it faces.

Author: Jenny Birch 51587

Job Title: Head of the Economic Crime Unit, Force CID

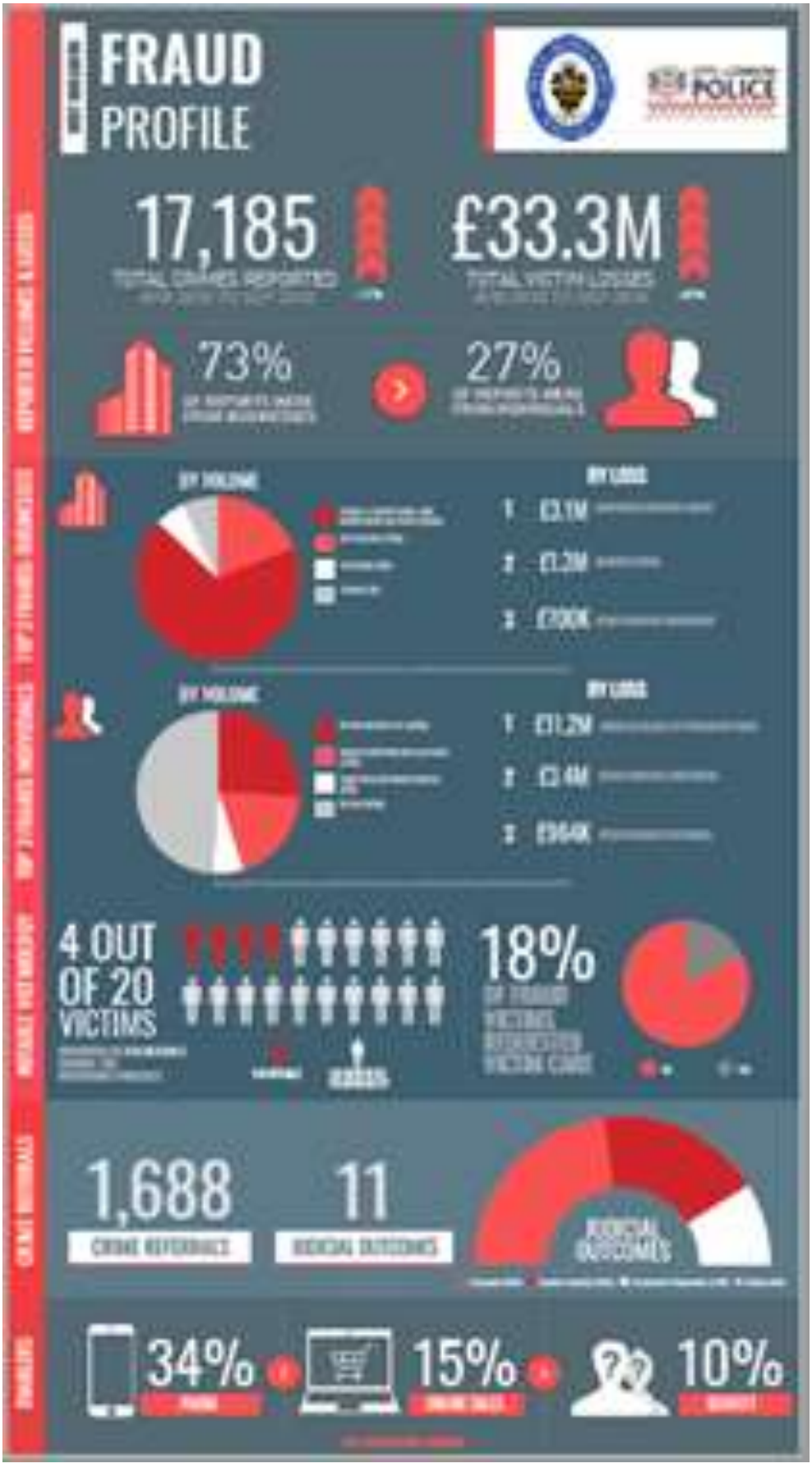
ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

APPENDIX A



ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

APPENDIX B – Latest WMP Fraud Dashboard



APPENDIX C – Latest WMP Cyber-Dependent Dashboard