| AGENDA ITEM | 8b |
|---|---|

**Strategic Policing and Crime Board**

**18 February 2020**

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

**Title:** *Fraud and Cybercrime*

**WMOPCC update presented by**: *Brendan Warner-Southwell*

**WMP update presented by:** *Jenny Birch and ACC Meir*

# OPCC Update

## Purpose of Paper

1. The purpose of this report is to provide the board with an update on the work being undertaken to develop the Police and Crime Commissioner's local and national fraud strategy.
2. This paper is for discussion and the board is asked to support the ongoing development of the work.

## Background

3. In the UK, the City of London (CoL) states that £2.2 billion was stolen from victims through fraudulent activity in the 2018-2019 financial year, with a reported 741,123 cases. However Experian, the credit rating agency, project the total cost of fraud to the UK economy to be closer to £190billion. In the West Midlands 35,964 cases were reported with a total loss of £58.8 million lost to victims in the same financial year. Given Experian's projections, the total impact of fraud on the West Midland's economy is likely to be much greater than that which is recorded.
4. The Fraud and Cybercrime paper for this month's SPCB breaks down in great detail what the fraud landcape currently looks like in the West Midlands. This paper will not look to reiterate the contents of that paper but will explain the advancments the OPCC is currently making both locally and nationally in advancing our response to fraud.

**Local Response to Fraud and Cyber Crime**

5. As an OPCC we have been working with both the Economic Crime Unit (ECU) and the ROCU Fraud team to discern where our office can add most support regarding West Midlands fraud victims. At present the ECU has recruited a Protect Co-ordinator. The OPCC is currently awaiting a formal business case so that we can explore further funding for this role

6. In September 2018 Outreach solutions were commissioned by Experian and the PCC's Office to deliver Fraud and Cyber Protect messaging to people over the age 55 across Birmingham. Outreach Solutions received £32,500 from Experian and £15,000 from the PCC's Office. The project utilised Age UK and Age Concern's links across the target area to feed information to the target cohort. The total numbers reached can be seen in the table below:

7.

| Type of activity | Target activity | Total activity |
|---|---|---|
| Community Events | 164 | 165 |
| No. of attendees | N/A | 2697 |
| One to Ones | 240 | 788 |
| Embedded One to Ones | 160 | 252 |
| Awareness Raising Venues | 212 | 222 |

8. The total number of people reached through the campaign was 3,737. Research undertaken on previous Tackling Fraud programmes, both independently and by Outreach Solution's supplementary research, shows that a programme of this type provides a significant reduction of losses to fraud and scams once individuals have the information they need to self-protect. Estimates point to a 8:1 return on investment ratio. By the time the programme had completed in May 2019, Outreach Solutions stated that they estimated the programme had saved people over age of 55 circa £380,000. It is stated that this saving will further grow over the next 12 months whilst the protect messaging material is further circulated amongst the Birmingham population.

9. The PCC hosted a Cyber Summit at Wolverhampton Science Park in November 2018 and was organised in partnership with WMP, ROCU and Get Safe Online. Topics included Mandate Fraud, secure disposal of data from business assets, Cyber Apprenticeships, the dark web, top ten tips to protect a business from cyber crime, and detecting social engineering. There were 4 workshops to enable a more in depth discussion later in the day. The day rounded off with a highly informative and enjoyable live hack of then APCC, now DPCC, Ashley Bertie's social media presence by Richard Plumb, a DOCO with WMP.

10. One of the most significant things that the OPCC has done locally in this space is establishing the West Midlands Fraud Board. This is a quarterly meeting that had it's inuagral meeting on the 27th of January 2020. The terms of reference were confirmed by group attendees at that meeting. The ambition of this group is two-fold. Firstly, to collaborate with the West Midlands Police and support them in the service they provide to the West Midlands public. The board meetings will give the Board space to understand the threat from Fraud in the West Midlands and to identify opportunities to strengthen the resilience of communities, support enhancements in the support of victims of fraud and

identify opportunities to influence government, businesses and other law enforcement partners both locally, regionally and nationally to ensure an effective response to fraud. The second ambition of the board is to provide a forum to discuss wider fraud Protect and Prevent programmes which can be developed across the West Midlands. The membership of the board will then be tasked with both the implementation and promotion of these programmes.

11. Current membership, as agreed in the terms of reference, stands at:

- Assistant Police and Crime Commissioner (Chair)
- West Midlands Police Assistant Chief Constable
- A representative from the West Midlands Fraud Forum
- A representative from the West Midlands Strategic Police and Crime Board
- An academic expert
- Head of West Midlands Police Economic Crime Unit
- An individual(s) who is an expert by lived experience
- A representative from WM Corporate Communications
- A representative from the City of London Police / National Fraud Coordinators Office
- Regional Fraud Coordinator
- A representative from the West Midlands Trading Standards group

12. Membership is due to be extended to a representative from the Crown Prosecuction Service and also a regional representative from CiFAS.

13. The OPCC will be running a 'Cyber Bootcamp' in partnership with WMP and the FSB on the 24th of March. The focus of the event will be to provide businesses across the West Midlands with the tools, learning and knowledge which will enable them to protect themselves against cyber crime. Participants will then be given a package of tools to take back into their organisations so that they can train their colleagues on how to defend themselves against cyber crime. The reasoning behind this being that organisations defences against cyber crime are only as strong as their most uninformed colleague.

**National Response to Fraud and Cyber Crime**

14. The OPCC is also focused on influencing the national agenda around fraud. The HMICFRS's report on fraud, published in early 2019, highlighted that focus needs to be given to the national response to fraud. This has been consolidated further by the government's Economic Crime Plan which was published in July 2019. This laid out specific actions which would be pushed at a governmental level to address fraud. Fraud is a topic which is gaining greater public scrutiny. The Times recent undercover story, which focused on the mistreatment of victims by Action Fraud staff, has made the public aware of the current failure of the national fraud strategy.

15. One aspect of the national strategy, the OPCC believes, which has not been given enough focus is the democratic governance functions currently in place. The democratic oversight for the national fraud strategy currently sits with the City of London Police Authority. No mechanisms are in place to communicate to other democratically elected police governors, PCCs, so that they can better hold their police forces to account and also the national strategy providers, the CoL Police. The PCC has been at the forefront of communicating this issue to other PCCs, the CoL Police, the CoL Police Authority and the Home Office. Initially concerns around fraud governance were communicated

through the APCC network through a letter, written on a collaborative basis between the other three OPCCs in the region. To gain wider recognition of our concerns, an article on the issue was collaboratively written between the Assistant Police and Crime Commissioner, Waheed Saleem, and the subject policy lead, Brendan Warner-Southwell, and was published in Policing Insight. Subsequently to that letter the OPCC met with the City of London Police and the City of London Police Authority, who both agreed that governance needs to be improved in this space. There needed to be clarity around responsibilities. The Police cannot take ownership for addressing everything when there are so many partners, both public and private institutions, trying to address the problem.

16. Subsequently to this the West Midlands OPCC and the Association of Police and Crime Commissioners made the joint decision to host a National Fraud Summit to get partners involved in this space to develop a series of recommendations which could be worked against nationally. Through creating a series of recommendations which have been worked on collaboratively, it is our hope that the recommendations we develop will carry far greater national weight.

17. This event will take place on the 20th of February 2020 at the Hyatt Regency Hotel. The day will be structured into two sections. In the morning we will hear from speakers, who are leaders in the fraud space from across policing, industry and also victims services. The second section will be facilitated by Birmingham City University who will conduct focus groups with the room attendees. Having an Higher Education institution conduct this function supports impartiality in this space. There will be three focus groups in total, focusing on: Fraud Governance, Fraud Victims Services and the Policing Response to Fraud.

18. After the summit a full findings report will be published by Birmingham City University, with a series of recommendations which can be worked against both locally and nationally.

19. It is our hope that through this process we will gain answers to the question of how we address the national fraud problem and justify ourselves in being able to lobby for these changes.

**Next Steps**

20. The board is asked to acknowledge the contents of this report and support our suggestions for advancing the PCC's Economic Strategy over the remainder of the PCC's term in office.

## West Midlands Police Update

### Purpose of paper

1. The purpose of this paper is to provide an update on how West Midlands Police (WMP) is building upon the fraud and cybercrime capability with the force. This paper is for discussion.

2. This paper will explain the fraud and cybercrime performance of WMP's Economic Crime Unit (ECU), the response to Her Majesty's Inspectorate of Constabulary and

Fire and Rescue Services (HMICFRS) thematic inspection of fraud[1], the response to the HMICFRS thematic inspection of cybercrime[2], partnership working and the key challenges facing the force.

**Background**

3. This is an update to the previous paper on fraud and cybercrime presented to the Strategic Policing and Crime Board in February 2019.

4. The Police and Crime Plan (2016-2020) recognises the damage to the social and economic fabric of our communities perpetrated by Organised Crime Groups (OCGs) and urban street gangs involved in fraud and a range of other serious offences.

5. The WMP ECU has the lead for fraud in the force, however fraud investigation is carried out by a range of teams both in the Force Criminal Investigation Department (FCID) and the Public Protection Unit (PPU).

6. The Police and Crime Plan also references the growing threat from cybercrime and the increased response required to address that threat. Cybercrime is categorised into two types: cyber-dependant[3] and cyber-enabled crime[4].

7. As with fraud investigation, there are a range of teams that investigate cyber-enabled crime both within FCID and other investigative departments. The ECU are the lead for cyber-dependent investigation.

8. Fraud and cybercrime reporting differs from other crime types as there is a national single point of reporting, Action Fraud. These reports are then triaged by the National Fraud Intelligence Bureau (NFIB) who are part of the City of London Police who are lead force for fraud.

9. Those reports deemed suitable for further investigation are then disseminated to the relevant agency, which includes the police, Department of Work and Pensions (DWP), and the National Crime Agency (NCA) etc. Typically reports are disseminated to geographical police forces based on where any identified offender resides and may relate to multiple victims targeted by the same offender or group of offenders.

10. Fraud can also be reported, by businesses, to Cifas[5] and UK Finance[6]. It is unlikely that any reports made to these agencies will be allocated to WMP for further

[1] Fraud: Time to Choose, An Inspection of the police response to fraud, April 2019
[2] Cyber: Keep the light on, An inspection of the police response to cyber-dependent crime, October 2019
[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 "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.
[5] Cifas holds the National Fraud Database (allows organisations to share data on thousands of fraud risk cases)
[6] UK Finance represents more than 250 firms across the banking and financial industry

investigation as either the financial institution itself will conduct an investigation and take appropriate action or it will go to another, more appropriate, law enforcement agency for progression such as the Serious Fraud Office.

**Introduction**

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

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

ii. **Investigation Management Team** (IMT) – Receive, assess and allocate for investigation, where appropriate, the referrals into WMP from Action Fraud and fraud related calls for service. The team perform the same function for any external referrals for banking enquiries received by way of International Letters of Request (ILORs) or European Investigation Orders (EIOs).

iii. **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 malpractice.

iv. **Cyber and Fraud Investigation Team** – Conduct investigations into complex cyber-enabled fraud and cyber-dependent crime. The team also receives, assesses and conducts investigation into the received reports of cyber-dependent crime.

v. **Protect Team** – Coordinates the force's Protect activity focussing crime prevention messaging to communities in the right way and upskilling WMP and partner agencies around the risk and threat from fraud and cybercrime. The team also incorporates the specialist Economic Crime Victim Care Unit (ECVCU) who provide bespoke victim support for victims of fraud and cybercrime working in conjunction with partner agencies.

vi. **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. This team also incorporates the newly formed Operation Pound team that seeks to proactively target individuals or groups involved in serious and organised crime, with a focus on drug dealing, with a view to disrupting their activity and seizing assets that can be shown to be the proceeds of crime.

**Performance**

*Fraud*

12. Due to the nature of fraud reporting, it is very difficult to get a complete understanding of the true nature of fraud committed against victims and businesses within the West Midlands area. One of the identified areas for development in the HMICFRS thematic inspection of fraud was the improvement of fraud recording and measurement across the country. Despite some improvements taking place in the latter half of 2019, there is still a gap in understanding the full picture.

13. The most accurate assessment of how WMP compares to the national picture is provided annually by NFIB and takes into account those fraud reports made to Action Fraud, Cifas and UK Finance.

14. The key findings from the latest annual assessment covering the 2018/2019 financial year are:

    i. The total number of reported crimes increased by 16% in 2018/2019 compared with the previous financial year. This is above the national increase, which was recorded as 9%. The majority of this crime is cyber-enabled, which concurs with the national picture.

    ii. The total loss to each victim has increased by 113.1%. This percentage is far higher than the national increase in victim loss (38.1%). This is likely to be within the business reported losses (see below) and work is ongoing to understand these losses and any underlying reasons.

    iii. The majority of victims continue to be businesses (71% of all reports).

    It should be noted that the Cifas and UK Finance figures skew this data considerably as the reports made to these agencies only come from businesses. As WMP hosts the headquarters of many of the major banking institutions, such as Royal Bank of Scotland and HSBC, many more business reports are made in this force area. This also affects the loss figures as business typically lose more money than individuals. When the WMP held data **alone** is analysed however, it shows that over the last 6 months 91% of fraud victims were individuals.

    iv. These businesses mostly fell victim to cheque, plastic card and online bank account fraud but suffered their biggest financial loss from corporate employee fraud and mandate fraud[7].

    v. Individual victims were most likely to be defrauded via online shopping and auctions or other advanced fee fraud[8] but suffered the biggest financial loss by abuse of position of trust.

[7] Mandate fraud is described as when a third party requests the victim to change a direct debit, standing order or bank transfer mandate, by purporting to be an organisation the victim is already connected with, for example a subscription or membership organisation or business supplier.

[8] Advance fee fraud occurs when offenders target victims to make advance or upfront payments for goods, services and/or financial gains that do not materialise

vi. 91 positive outcomes, equating to 4% of NFIB disseminations, were reported in 2018/2019. The national figures indicate an outcome rate of 18%.

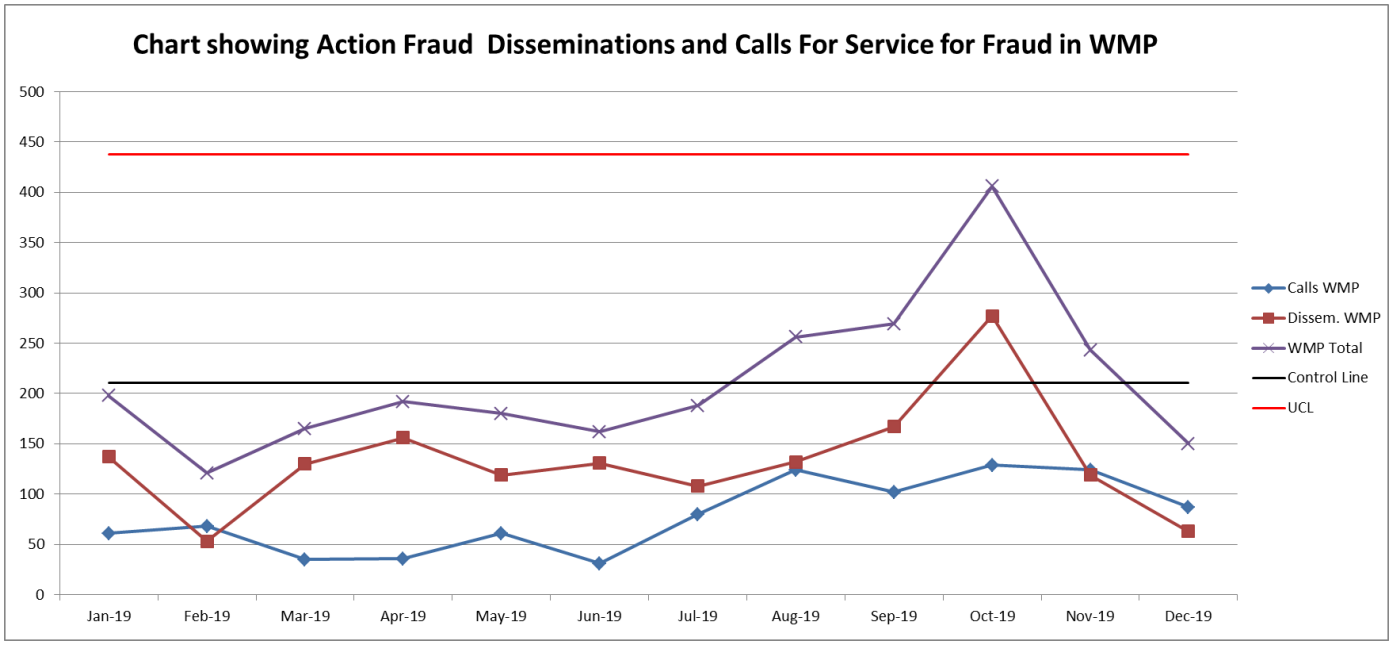
This low outcome rate is due to a number of factors. Firstly, the WMP process for returning outcomes to NFIB has been flawed in that the procedure for resolving nationally allocated crime numbers (known as NFRC numbers) with local non-crime numbers has not been rigorous enough to ensure that the returns were 100% accurate. The unit recruited an intelligence analyst in April 2019, and because of their insight and work in this area, a change in procedure has been made to address this failing and, whilst it remains a work in progress, the figures are improving. For example, the outcome rate for December 2019 was at 10%. The second factor impacting on the outcome rate, is the nature of fraud investigation and the length of time it takes 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.

The summary of the annual assessment can be found at Appendix A.

15. A comparison between most similar forces is currently difficult to achieve as there is no shared dashboard that would allow easy access to such data. In addition each force is organised in a different way i.e. will have a different approach to the investigation of the NFIB disseminations versus the fraud related calls for service and have different performance measures to which they are working.

16. Despite the described data limitations, the ECU holds an internal monthly performance meeting where the performance of each of the teams within the unit is analysed, discussed and any barriers to performance identified. Actions are then raised to address these barriers as far as is possible.

17. In terms of incoming demand, as shown in the graph below, the number of NFIB disseminations and fraud related calls for service have steadily increased over the last 12 months peaking in October 2019 and then reducing over the final two months of the year. It should be noted that one dissemination, and therefore one WMP held non-crime number, may in fact relate to multiple victims.




18. In May 2019, the ECU undertook an assessment exercise[9] to determine the key fraud types that posed the greatest risk to the West Midlands area. These key crime types would then assist in the prioritisation of resources and protect activity as necessary. The priorities for 2019/2020 are:

    i. **Computer Attack** (hacking)

    In comparison with the preceding financial year, the monthly averages for this fraud type remain largely stable

    ii. **Deception** including employee, application and mortgage fraud as well as bogus salesperson, dating scams and ticket fraud

    In comparison with the preceding financial year, the monthly averages for this fraud type have been decreasing with the exception of ticket fraud (which is increasing to an average of 27 reports per month)

    iii. **Cheque, Plastic Card and Online Bank Account fraud**

    This crime type continues to increase year on year with an increased average of 105 reports per month.

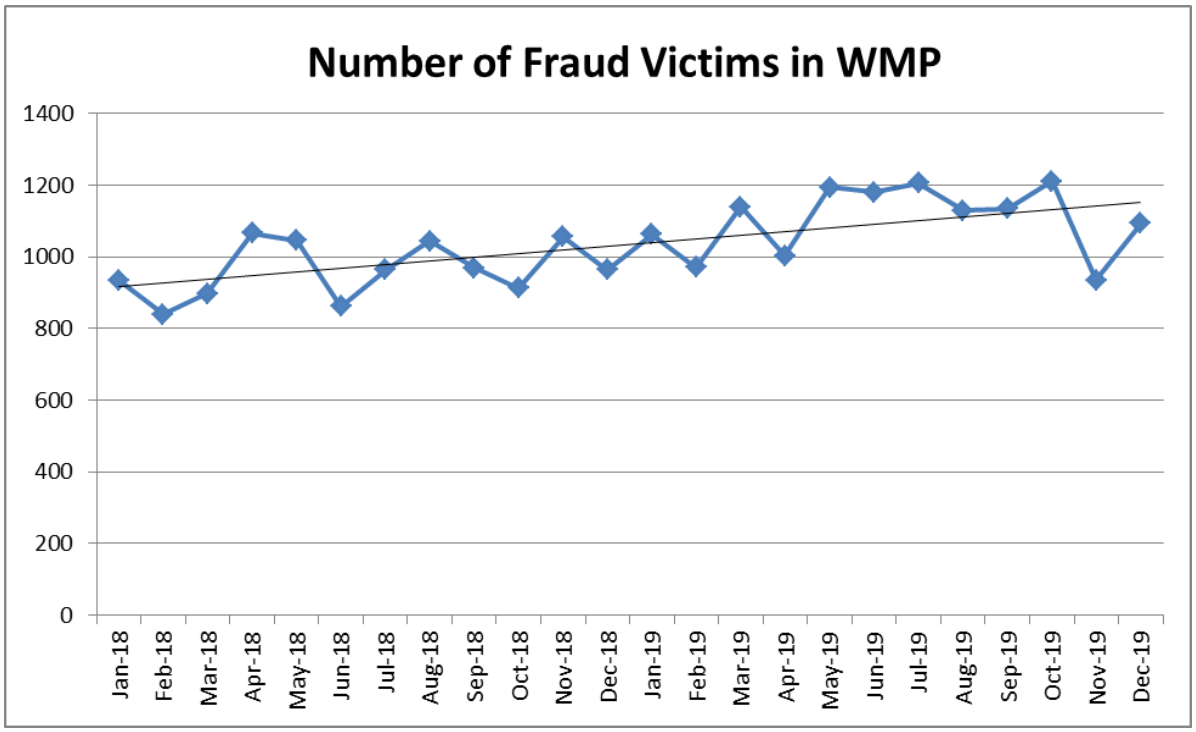
19. Within the ECU performance meeting, these priorities are reviewed and any emerging trends are highlighted. For example, online shopping and auction fraud has continued to increase year on year to an average of 237 reports per month and presents a particular seasonal risk in the run up to Christmas. As a result of this analysis, protect activity was put into place to warn shoppers of the risk of this type of fraud including tips on how to prevent themselves from becoming a victim.

[9] This assessment used historical data sets (over last five years) coupled with a risk assessment of each crime type using the strategic Management of Risk in Law Enforcement (MoRiLE) tool

20. These priorities will be reviewed annually to coincide with the start of the new financial year.

21. Not all fraud reported to Action Fraud is disseminated as it may be filed at source if there are no active lines of enquiry. In order to assist forces' in understanding their fraud victim profile, NFIB publish weekly lists of anonymised victim data.

22. From this data we are able to show, as per the below, the numbers of victims of fraud who are resident in the West Midlands area. The graph shows that, in line with the increasing number of reports over the last 12 months, there is an increasing trend in the number of victims. For example, the average number of victims per month in 2016 was 751 compared with 1,107 in 2019.




23. As discussed in paragraph 14(iii) above, in the last 6 months according to WMP data, 91% of the victims of fraud reported to WMP were individuals as opposed to businesses. The average loss for each individual was in the region of £50,000. However 44% of these victims reported zero loss. This information is used as an indirect measure of success of the Protect strategy as the more victims who recognise a potential fraud and report accordingly but refuse to pay the fraudsters the better.

24. WMP held data indicates businesses on average suffered far fewer losses than individuals, totalling in the region of £27,000 with zero loss reported in 37% of cases.

25. In terms of the outcome decision for those offences reported or disseminated to WMP, the IMT are now filing around 20% of the reports received. Filing will only take place after the report has received sufficient investigation to confirm that no

further reasonable and proportionate actions can be taken that would warrant allocation to an investigation team or referral to a more relevant partner agency. This is an improvement to the figures reviewed by HMICFRS as part of the thematic inspection for fraud that estimated that the filing rates were much higher.

26. The IMT will also ensure that if no further investigation is to take place, all reasonable avenues for disruption are explored such as the issuance of "cease and desist" letters, submission of intelligence, application for website suspensions and the use of out of disposal options such as conditional cautions. Performance monitoring for 2020 will now include an analysis of these disruption techniques in order to identify best practice and further help to shape the response to fraud.

27. Of those reports that do get allocated for further investigation, the majority are retained in the ECU as they are of sufficient seriousness and complexity to warrant in-depth investigation. For example in December 2019, 58% of the fraud offences crimed in this month were retained by the ECU with the remainder being allocated to the geographic investigation teams with FCID and, where there is a domestic or vulnerable adult abuse footprint on the investigation, to the PPU. This distribution of investigation is also monitored closely in the monthly ECU performance meetings.

28. As referenced in paragraph 11(ii), the unit is the single point of contact for all ILORs and EIOs that come from law enforcement agencies across Europe and the world, requesting banking information in support of a range of investigations including fraud. The chart below shows that in the last 12 months the number of these requests is increasing, adding to the demand on the unit.

29. An example of the investigative work that the ECU undertakes is the conviction of a Birmingham City Council (BCC) worker of fraud by abuse of position; the fraud type with the highest loss to individual victims. The offender in this case was employed by BCC in the Appointee and Court Deputy Service (ACDS) team. This team maintains court appointed financial responsibility for vulnerable, elderly persons residing predominantly in care homes.

30. Over a period of 18 months, the offender used their position to access up to £270,000 from the bank accounts of over 20 elderly care home residents. This came to light when new management took over the ACDS team and reviewed the team's processes. Fortunately, BCC compensated all victims immediately.

31. The Complex Fraud Investigation Team liaised with BCC and the BCC's safeguarding team agreed they would take primacy for the welfare of the victims and family liaison. Due to the health care needs of the victims, they were unaware of their initial loss but their families were equally supported by the BCC safeguarding team. The team regularly updated BCC as the investigation progressed to make sure the victim's families had as much information as possible.

32. The offender was arrested following a warrant executed at their home address. Following a lengthy investigation process, the offender was charged with multiple offences of Fraud by Abuse of Position. They pleaded guilty in February 2019 during the initial weeks of the crown court trial and was subsequently sentenced to four years imprisonment.

33. A financial investigation into the offender ran in parallel to the criminal investigation and upon conviction, Financial Investigators from the ECU obtained a confiscation order under the Proceeds of Crime Act to value of £190,000. The financial investigation could only trace £60,000 of assets belonging to the offender, which was the initial amount the offender was ordered to repay. However the order will remain with the offender for life until it is fully repaid.

*Cybercrime*

34. NFIB produced an annual profile of cyber-dependent crime in the West Midlands covering The key findings from this assessment are:

    i. The total number of reported crime increased by 3.5% in 2018/2019 compared with the previous financial year.

       The majority of this crime is hacking related (hacking of social media and emails). Indeed hacking continues to represent the greatest threat from cyber-dependent crime both by volume and loss with £2.6M lost in 2018/2019 due to this offence type.

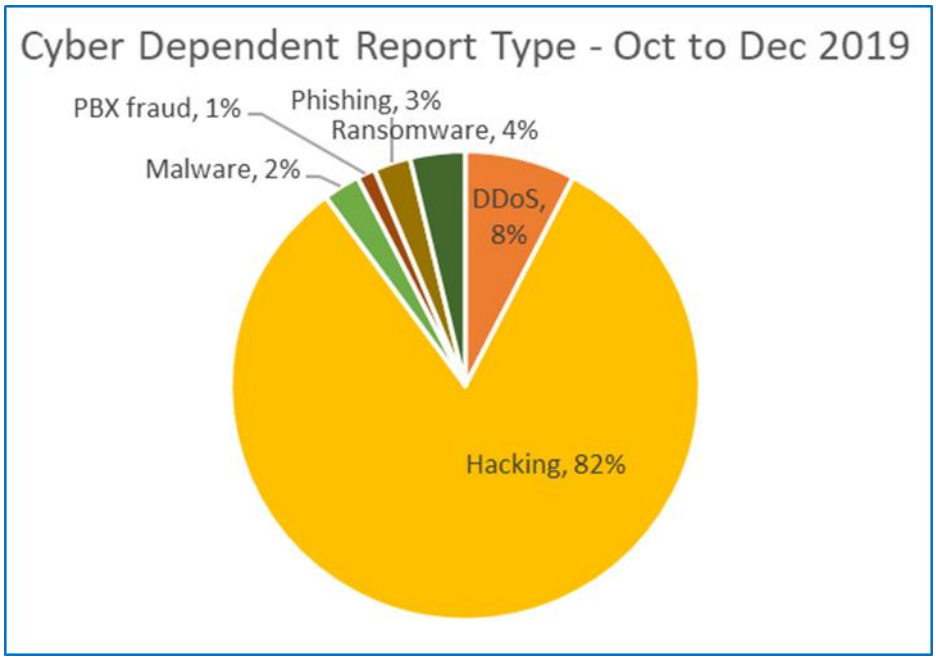
    ii. The total loss to each victim has increased by roughly 74%.

    iii. The majority of victims continue to be individuals (89% of all reports) and this is mirrored in the national picture.

The summary of the annual assessment can be found at Appendix B. Unfortunately a national comparison to this data was not available at the time of writing.

35. Locally held data for this financial year shows the varying numbers of cyber-dependent crime reports received by WMP month on month, but confirms that hacking still presents the greatest risk to victims.

| Month (2019) | No of Cyber reports |
|---|---|
| April | 20 |
| May | 15 |
| June | 32 |
| Jul | 16 |
| Aug | 13 |
| Sep | 22 |
| Oct | 32 |
| Nov | 28 |
| Dec | 25 |




36. There is a nationally agreed performance framework for cyber-dependent investigation, that sets out four Key Performance Indicators (KPIs) as below:

    i. 100% of Action Fraud referrals will be investigated

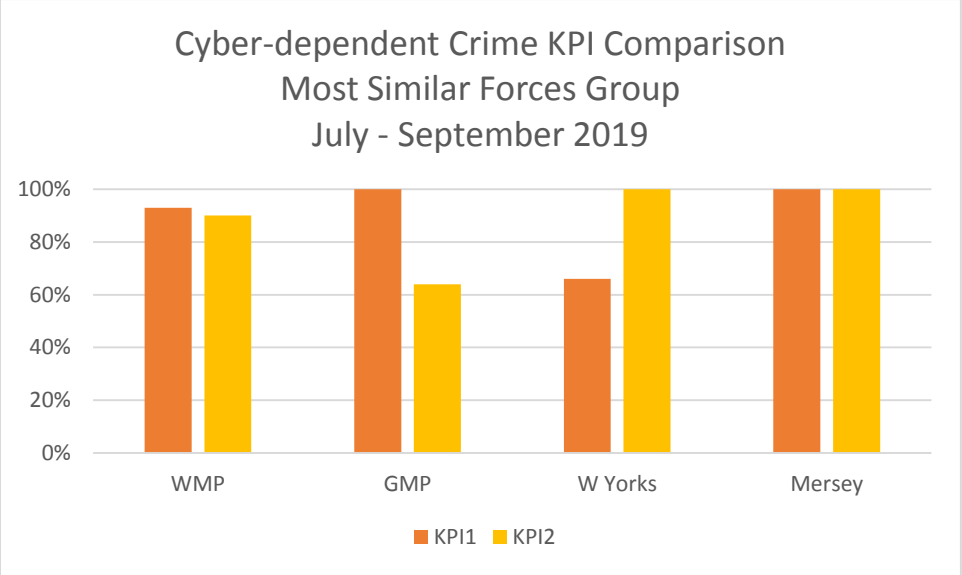
    ii. 100% of victims who report to Action Fraud will get advice in person or over the telephone to prevent them becoming repeat victims

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

    iv. 75% of organisations who receive prepare[10] advice will develop or review incident response plans and test them

37. Comparative performance between WMP and the most similar forces group for the period July to September 2019 against the first two KPIs can be found in the graph below[11]. The national average for each of these KPIs is 94%.

[10] Defined as activity designed to assist in the preparation for when crime occurs and to mitigate the impact
[11] Source: National Force Specialist Cyber Project Q2 Performance Report, July – September 2019




38. Whilst the performance of WMP appears, on the basis of the above data, to be under the national average and short of the expectation levels described by the KPIs, there are a number of reasons for this:

    i. Typically cyber-dependent disseminations from NFIB take the form of a weekly spread sheet sent to each force. An exception to this is the report of a crime in action where the offending is happening in real time and not reported retrospectively. Crimes in action are disseminated immediately to WMP and action is taken as soon as possible.

    The monthly returns submitted to the Regional Cybercrime Coordinator often do not include those cases disseminated that week on which the team are still working, and therefore the team are unable to report that all of the reports received that month have been actioned in accordance with the KPIs.

    ii. An increasing number of the reports received from NFIB are subsequently determined not to be an offence and therefore do not receive any investigation. For example, a number of victims (10 since October 2019) suffer from mental health issues that led them to believe they have been the victim of cybercrime, whereas there is no evidence that this the case. In such cases as these the victims are referred through to the Mental Health Community Team or their own doctors.

    iii. Some victims who report their offences to Action Fraud will not respond to any further attempts at communication by WMP and once all reasonable steps have been taken to make that contact, the case is filed with no further action taken. This prevents both an investigation taking place and the victim receiving appropriate protect advice.

39. The performance of the Cyber and Fraud Investigation Team in respect of investigation and victim advice is monitored closely via the ECU monthly performance meetings.

40. It has proved to be very difficult to gather data in relation to KPIs three and four (paragraphs 36(iii) and (iv) respectively) as often once the threat of the cyber-dependent crime has passed, victims have no further wish to communicate with WMP. However the Cyber and Fraud Investigation Team continue to try to gather the information necessary by way of an easy to complete survey.

41. WMP ECU continue to contribute the national debate about cyber-dependent performance measurement via the Regional Cyber Leads meeting and via the Regional Cybercrime Coordinator.

*Cybercrime Case Study*

42. Between January and March 2019, a college within the West Midlands was subjected to a number of distributed denial of service (DDoS) attacks which have caused various service outages. This type of attack is one of the most commonly used, and usually against company websites and is often extremely hard to prevent, track, and stop. DDoS services can also be purchased in the form of 'web-stresser applications' and so the person directing the attack does not have to actually have the technical capability to direct an attack. A 'stresser application' or an 'IP stresser' is a tool designed to test a network or server. If a Stresser tool is used against another individual or a company/organisation's network or server which would ultimately result in 'Denial-of-Service', then this would be deemed illegal.

43. The outages have resulted in lost Internet and e-mail access (all staff and students on all campuses) leading to exams being cancelled and temporary loss of access to server resources (college data stored in the cloud). For a college, frequent exam rescheduling risks escalating costs and increasing reputational damage.

44. Initially the college was unable to detect where the attacks originated as they had a single external IP address that related to all of their buildings. They then changed the external IP address that staff/students use on the Internet, when coming from different buildings and networks. Any attack with a destination of one of these new IP addresses would tell them from where the instigation of the attack was coming. As a result of this, a particular location identified as the site where most of the attacks appeared to originate. Eventually there was an attack where only one device was connected to that network used by a particular student who was subsequently identified.

45. On a day before one of the attacks, a device that same student was using was discovered to have browsed a 'Stresser' website. This was the only occasion in 2019 where an individual, in the whole of the college (staff and students), was found to access a Stresser site.

46. The student was invited by the Cyber and Fraud Investigation Team to come in for a voluntary interview and admitted the offence as they had wished to not sit their examinations. The student received a conditional caution for the offence and was

referred into cyber prevention pathways established by the Regional Cybercrime Unit. They must complete the training and education programme and commit no further offences in order for the conditions of the caution to be satisfied or else risk entering the criminal justice system.

**Victim Care**

47. The ECVCU are part of a City of London Police led pilot into the improvement of victim care for victims of fraud. The role of the WMP ECVCU is to provide support to those victims of fraud and cybercrime who are assessed by the National ECVCU as requiring face to face support focussed on safeguarding the most vulnerable at risk individuals. The team also take any referrals made by any member of WMP where they feel that a victim requires that level of support. For example, the ECU Proactive Investigation Team regularly identify and refer potential vulnerable victims from their review and assessment of the suspicious activity reports the force receives.

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

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

    ii. Referral service to partners to further support the victims e.g. Mental Health Services, Social Services, and Age Concern UK etc.

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

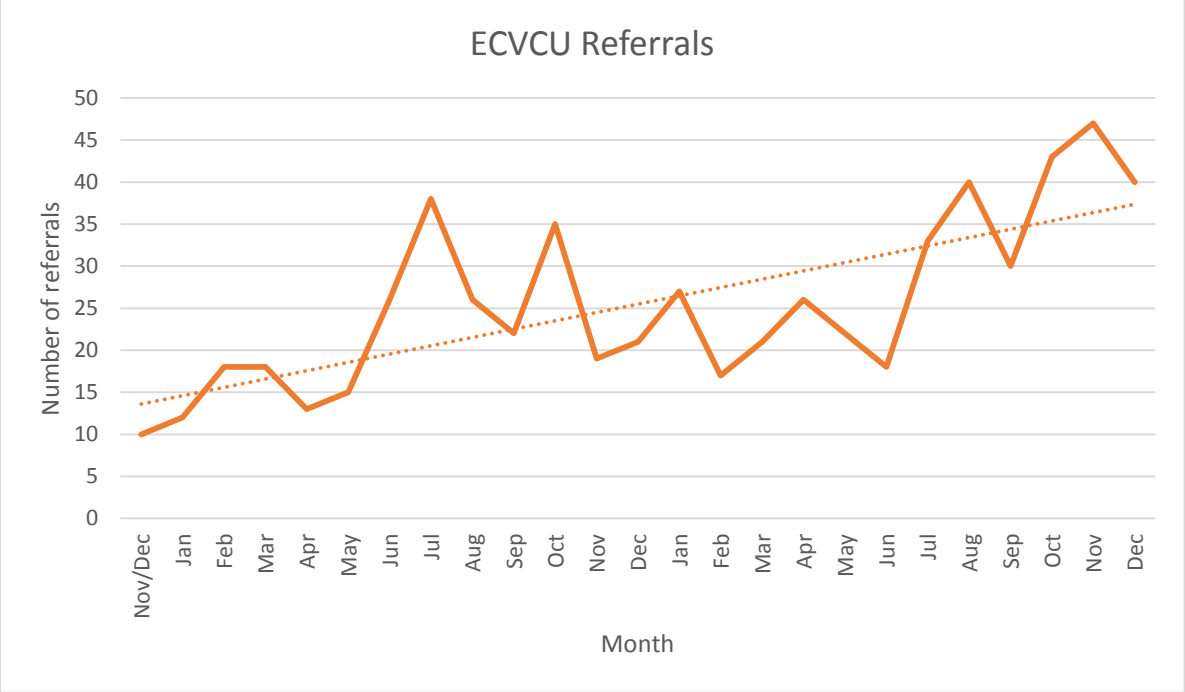
    iv. Liaison with Action Fraud and NFIB to discuss the progress of their case and to explain the crime recording and investigative process

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

    vi. 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 continues to be funded from the WMP Asset Recovery Fund, generated from financial assets recovered under the Proceeds of Crime Act.

49. The team comprise of two Detective Constables (DCs), allocated from the main ECU establishment, and have recently moved under the leadership of the ECU Protect Coordinator. The team work alongside three volunteers from the community who are working with Victim Support to provide a service to victims of fraud. A review of the ECVCU process and team is ongoing to ensure that all opportunities to provide victim support are maximised.

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




51. The WMP ECVCU are sent victim referrals for all those victims of fraud who are under 18 years for triage. NFIB, due to the victim's age, do not offer any support or guidance if they have been the victim of fraud. A lot of these victims are low level in term of amount lost, but in relation to their income the loss can have a devastating effect on the individual.

52. The team will contact all of these victims and offer any support and help possible. Normally in the first instance that will be by phone/letter or email, but dependant on individual circumstance visits maybe required for further assessment and safeguarding or signposting. The ECVCU has engaged with schools, colleges and universities around safeguarding and intelligence gathering and disruption, especially with regards to money mules[12].

*Victim Care Case Study*

53. The WMP ECU received a referral from the National ECVCU regarding a victim who had been approached on numerous occasions by various offenders who were involved in a sophisticated advanced fee fraud. The victim had been duped into paying thousands of pounds in the hope of inheriting millions.

54. The team visited the victim's address with the victim's adult children present. Due to the debts they had accrued, the victim had been forced to sell their home and move in with their children. The children then became concerned that creditors would attend their home seeking the money they were owed. In addition, the victim had recently been diagnosed with dementia.

[12] A money mule is s a person who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically, on behalf of others. Typically, the mule is paid for services with a small part of the money transferred.

55. The team had several meetings with the family but the victim refused to believe that they were the victim of a fraud. The team have tried all options to prevent the victim from continuing to pay the offenders more money but to no avail and the victim refuses to discuss the matter with his family.

56. Despite this, the team continue to provide support safeguarding and emotional support to the victim's children.

57. Unfortunately this victim's story is not unique. The Think Jessica charity[13] was started by the daughter of an elderly victim of postal fraud. Jessica was targeted by fraudsters who, via the "junk" mail many people throw away, offer the receiver a lottery or prize draw win in return for a release fee. Jessica became obsessed with her mail and lost all of her savings, often going without food so that she could pay the money requested in the letters she received. She died refusing to believe that she was the victim of fraud. The Think Jessica charity closed in October 2019 but still provides educational material to help combat this type of fraud. The ECU are utilising this material by distributing directly to victims of crime and in the wider awareness work in which the team regularly engage.

*Protect Coordination*

58. The ECU recruited its first police staff Protect Coordinator in September 2019. The purpose of the role is to coordinate the force's response to the victims of fraud and cybercrime.

59. The post is for a fixed term and is part funded following a Police Transformation Fund bid by the National Cybercrime Project. The funding for this role has now been confirmed until March 2021.

60. The coordinator is working to an overall strategy to achieve the following in relation to fraud and cybercrime:

    i. Establish who and which areas of the force are most at risk of becoming victims

    ii. Reduce the number of victims

    iii. Improve support to victims

    iv. Identify who are likely to become enablers for this type of e.g. money mules

    v. Increase awareness and understanding across policing

    vi. Lead and support awareness campaigns for the wider community to promote the understanding of the risks presented by this type of offending and how to protect oneself against it

[13] https://www.thinkjessica.com/

vii. Further develop ECU partnership with third sector, partner and other law enforcement agencies.

61. An example of the work the Protect Coordinator is undertaking is in harnessing the Police Community Support Officer (PCSO) network to undertake bespoke fraud and cybercrime protect activity on each of the eight neighbourhood policing units within WMP. The network currently consists of 15 PCSOs with a further seven waiting to receive the initial training[14].

62. The coordinator is also leading the protect response to Operation Radium. Operation Radium is the first of four periods of fraud intensification led by the City of London Police under the auspices of Project Otello. The focus of Operation Radium is courier fraud[15]. The Protect Coordinator has been working with Trading Standards, West Midlands Fire Service, Age UK and the PCSO network in order to ensure that key messaging and educational material is distributed to the right areas to raise awareness.

63. As referenced in the performance section above (see paragraphs 21 and 22), NFIB produce weekly lists of all of the victims who have reported an offence to Action Fraud. In the past, the ECU use of these lists was limited however, the unit has recently taken on board best practice from Staffordshire Police regarding the use of this data. The Protect Coordinator in conjunction with the IMT and ECU analyst will now:

i. Make contact with the victims within that week who have lost the most amount of money to assist them in retrieving the money via the relevant banks or financial institutions if this is possible

ii. Review the top five businesses each week and work with the WMP Business Crime Coordinator to make a contact plan for those businesses to make sure they receive appropriate tailored protect advice to prevent further victimisation

iii. Increase the referrals into the ECVCU by identifying the victims on the list who are deemed vulnerable by the NFIB led vulnerability threat matrix. The identified vulnerable victims will be cross referenced with referrals already made by the National ECVCU to ensure that no victim is contacted twice in error.

iv. Map the victims and overlay with the force impact areas[16] in order to utilise the ongoing activity in these areas and the PCSO network to address fraud and cybercrime offending in these key areas.

[14] 5 from Birmingham East, 7 from Birmingham West, 3 from Coventry, 1 from Solihull, 2 from Dudley, 1 from Sandwell, 2 from Walsall and 1 from Wolverhampton

[15] Courier fraud is when a fraudster contacts victims by telephone purporting to be a police officer or bank official and after trust has been established, suggests a plausible reason why the victim should go to the bank and take out money (or withdraw it from a bureau de change or buy an expensive item). A courier will then come to collect the money or item with the promise of reimbursement that does not occur.

[16] Impact areas make up around 4% of the Force geography but account for 20% of total recorded crime and 30% of homicides. The areas are being tackled by the whole of WMP in order to reduce crime and protect the public.

**Response to HMICFRS Recommendations**

64. In April 2019, HMCIFRS published the results of the thematic inspection of fraud. Within this document there were several recommendations for the National Police Chiefs Council Coordinator for Economic Crime and two recommendations for forces, which are:

    i. Ensure processes are in place to accurately and efficiently report fraud outcomes to NFIB

    As referenced in paragraph 14(vi) above, after a lapse, the correct processes and monitoring is now in place to ensure accuracy in the outcome data being submitted to NFIB each month.

    ii. Publish force policy for responding to and investigating allegations of fraud

    Both the investigative and overall WMP Fraud strategies have been signed off at the Crime Governance Board and are awaiting publication via the force's internet site.

65. In addition to these recommendations, there were five identified areas for improvement:

    i. Improve the way the force uses the National Fraud Intelligence Bureau monthly victim lists to identify and support vulnerable victims and others who require additional support

    This is being completed (please see paragraph 63 above).

    ii. Improve the identification and mapping of organised crime groups in which the principal criminality is fraud

    The unit has been successful in its bid to map three fraud related organised crime groups since January 2019 with a further three under consideration.

    iii. Ensure that fraudsters are included among those considered for serious organised crime 'prevent' tactics, including by local strategic partnership boards and through integrated offender management processes.

    The WMP Fraud strategy sets out the ambition to utilise the existing offender management structures and to work with external partners, such as the local adult safeguarding boards, to tackle fraud offending where possible. This work is currently in its infancy.

    The prevent aspect of fraud offending remains largely unexplored. There is a deficit in understanding the drivers and trigger factors that create fraud offenders and therefore make diversionary activity difficult to source. The unit is working with the Risk-Assurance and Organisational Learning Team with a view to commissioning academic

work to help to understanding fraud offending. The unit is also engaged in conversation with the Office of the Police and Crime Commissioner in order to enlist their support to identify referral pathways for fraud offenders.

iv. Increase their force's use of ancillary orders against fraudsters

The unit has one active Serious Crime Prevention Order in place and consistently considers this as an option for all offenders convicted of serious and complex fraud offences in conjunction with the Crown Prosecution Service.

The unit is currently exploring the use of civil orders such as the use of community protection warnings and notices and criminal behaviour orders.

v. Ensure compliance with the Code of Practice for Victims of Crime when investigating fraud.

Dip samples are completed once per quarter to ensure compliance with the victim's code. The results of the dip samples are fed into the ECU monthly performance meetings for action as appropriate. The unit is also engaged in the Force Victim Champion meetings.

66. In October 2019, HMCIFRS published the results of the thematic inspection of cyber-dependent crime. Within this document there was one recommendation for the National Police Chiefs Council lead for cybercrime and Coordinator for Economic Crime and one area of improvement for Forces, which is:

i. Chief Constables should evaluate the use that their force makes of cyber specials and volunteers to ensure that they are used effectively.

The ROCU are taking the lead for the West Midlands regional forces in response to this area for improvement.

**Partnership Working**

*External Partnership*

67. The ECU are involved with various partners across the West Midlands in order to refer, receive and support fraud and cybercrime investigations. The unit also seeks to share expertise and best practice between all relevant agencies.

68. The ECU continues to lead the force response to the banking protocol[17] and working with Trading

| Month | No of Banking Protocol Logs | No of resultant offences |
|---|---|---|
| Jun | 62 | 18 |
| Jul | 63 | 14 |
| Aug | 49 | 16 |
| Sep | 42 | 9 |
| Oct | 57 | 13 |
| Nov | 65 | 13 |
| Dec | 45 | 10 |

[17] The protocol is an initiative ls. Its aim is, at the earliest opportunity, to identify vulnera s from their bank accounts by unscrupulous criminals and to

Standards in order to protect victims of fraud and prevent loss. The table below shows the number of banking protocol incident logs created and the number of resultant offences (which average 24% of the total number of logs created).

69. The unit continues to work closely with our partners in DWP, Her Majesty's Revenue and Customs (HMRC), the Insurance Fraud Bureau, the NHS Fraud Teams and the NCA, often engaging in joint operations.

70. The ECU have continued to develop the relationships the unit has with the major financial institutions such as Santander, Lloyds Bank, Barclays Bank and the Coventry Building Society. The unit have received operational referrals from these institutions that are being investigated.

71. The unit is also currently working with colleagues from the European Anti-Fraud office and UK Research and Innovation funding agency regarding the potential criminal practice of companies who have been successful in their bids for both European and UK business funding.

72. The ECU continues to be a strategic board member and supporter of the Midland Fraud Forum. 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.

*Internal Partnership*

73. As noted in paragraph 5 above, the ECU is the lead for fraud and cyber-dependent crime in the force. As such, the unit has responsibilities for raising awareness and training relevant teams across the force area in relation to fraud and cybercrime. The team are involved in delivery of training and continuous professional development inputs to Force Contact, new student officers, the PCSO network and the wider FCID department.

74. The unit also arranged for the in-house delivery of the Economic Crime Academy Volume and Priority Fraud investigation and Accredited Counter Fraud Managers

courses. Participants for these courses came from within the ECU, the wider FCID, PPU and colleagues from the West Midlands regional forces.

75. The team regularly provide advice and guidance to other investigative teams that hold fraud investigations to assist in achieving the best outcome. The team also provides officers and staff when requested to assist other areas of business facing critical demand such as in relation to homicide and domestic abuse.

76. The ECU has a good working relationship with the ROCU and have been successful in various bids for regional asset support in a number of investigations. The unit is also working with both the regional coordinators for fraud and cybercrime in order to improve working practices learning from national best practice.

77. The unit also maintains a good relationship with the Operations department who have been very supportive in assisting in the delivery of support to enforcement activity.

**Key Challenges and Future Opportunities**

78. The key challenges facing WMP remains the volume of fraud and cybercrime reports made and disseminated to the force and the complexity of fraud and cybercrime investigation. This complexity comes from a range of factors including increased sophistication in *modus operandi*, the use of money mules (disguising the real perpetrators of the offence) and the fact that these offence types transcend geographical boundaries making enquiries more difficult and complicated.

79. The focus for the future must therefore be around the prevention of victimisation both in terms of the reduction in harm and loss to victims, including businesses, and in terms of demand suppression.

80. The work of the Protect Coordinator will be pivotal in helping achieve this objective and the unit are exploring ways to provide greater resilience to the Protect Team and the Coordinator in particular.

81. As technology gets more sophisticated and offenders find more imaginative ways to defraud victims and commit cybercrime, a real challenge facing the ECU is keeping up to date with the changing criminal techniques. Continuous learning and development opportunities are being sought balancing the need for training versus the cost. This is especially true in relation to cyber-dependent crime and the unit have been the recipients of much needed national project funding to help to ensure that the Cyber and Fraud Investigation team are sufficiently trained and equipped to complete their work.

82. Cryptocurrency also poses a challenge not only to fraud investigation but also to more general financial investigation and asset recovery. The unit was successful in a bid for funding from the WMP Asset Recovery Fund to obtain a three day cryptocurrency training course that was delivered to members of the ECU in

addition to colleagues from the Digital Media Team and ROCU. There are also plans to deliver shorter cryptocurrency awareness sessions to colleagues in the wider force, such as in Neighbourhood Task Force teams and Force Response, to increase their understanding of what cryptocurrency is and what to look for when they are deployed.

83. The team are also in receipt of funding to purchase equipment to allow for the seizure and retention of cryptocurrency. Work is ongoing to complete a WMP cryptocurrency policy in conjunction with regional colleagues.

84. Following an exposé of working practices within Action Fraud by The Times, Sir Craig Mackey was commissioned to conduct a review of Action Fraud. He has recommended that the service around fraud should now be "re-defined and brought back into line with industry standards and public expectation"[18]. It is expected that Sir Mackey's report will change the landscape for the reporting, management and investigation of fraud and is currently being considered by the Home Office.

**WMOPCC Author:** Brendan Warner-Southwell

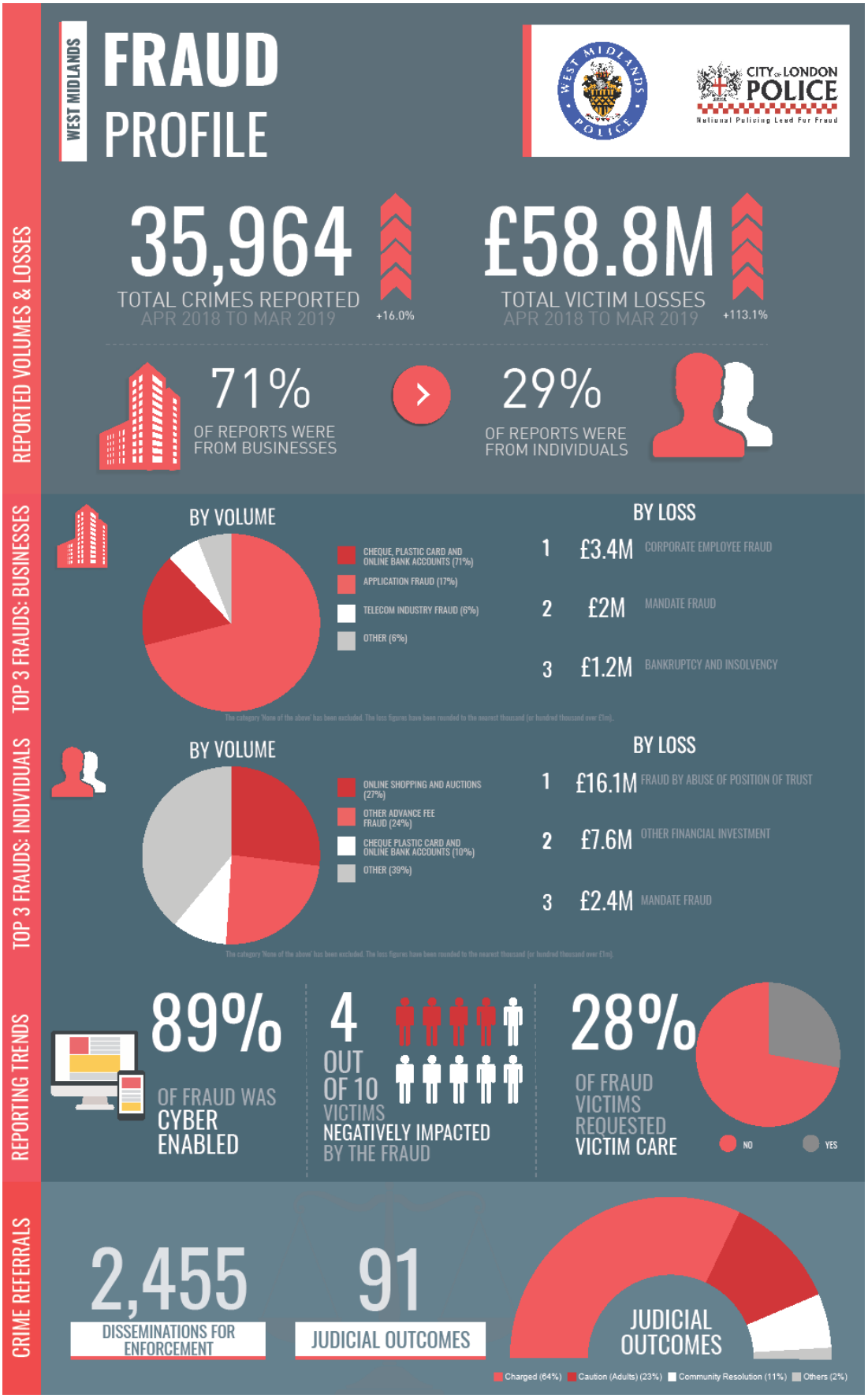
**Job Title:** Policy Officer

**WMP Author:** Jenny Birch

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

[18] https://www.bbc.co.uk/news/uk-51246926

## APPENDIX A – Latest WMP Fraud Dashboard



## APPENDIX B – Latest WMP Cyber-dependent Crime Dashboard