DORSET POLICE & CRIME COMMISSIONER

AGENDA NO: 9

DORSET POLICE & CRIME PANEL – 10 DECEMBER 2020

FRAUD AND CYBER CRIME

REPORT BY THE CHIEF EXECUTIVE

PURPOSE OF THE PAPER

This paper updates members on the Police and Crime Commissioner's work to continue to seek appropriate responses to the fraud and cyber-crime threats most affecting the people of Dorset.

1. INTRODUCTION

1.1 Nationally, there have been more than 340,000 reports of fraud or cyber-crime made in the last 12 months, and £1.9bn has been lost. The volume, rates, and trends of crime impacting Dorset is (as far as can be seen with locally available data) in line with the national picture, and here in Dorset, over the same period, a little over 4,200 reports of fraud or cyber-crime have been made, with nearly £17m lost in the county.

1.2 Both nationally and locally, online shopping and auction scams are the biggest type of crime, but there are many other types of scams and fraud that are a concern, largely relating to cheque, plastics and online account fraud not relating to the payment service provider.

1.3 Fraud and cyber-crime are globalised and cross-border, with the reach of fraudsters extended due to the use of new technologies, meaning that the victims and offender are often quite remote from each other. Such crimes are best tackled by policing capabilities that match the scale and range of operations as the criminals themselves and, therefore, the policing structures that deal with fraud and cyber-crime (often referred to as 'economic' crime) are largely national, as follows:

Action Fraud (take reports)
Action Fraud receives all fraud and cyber-crime reports from members of the public, and functions as the UK's national reporting centre (excluding Scotland). It provides a centralised point of contact for information about fraud and financially motivated internet crime and is run by the City of London Police working alongside the National Fraud Intelligence Bureau (NFIB).

National Fraud Intelligence Bureau (assess reports)
The NFIB receive all Action Fraud reports and are responsible for assessing these and ensuring they are investigated by the correct agency. They analyse reports received, investigate emerging trends and sift through actionable intelligence to build crime packages which they then pass to national, regional and local policing agencies for further work.

City of London Police (national supporting role and high harm investigations)
City of London are the national policing lead for economic crime, and provide specialist support and guidance to Action Fraud, the NFIB, and to police forces, other law enforcement agencies, and industry. They are also responsible for carrying out investigations for those frauds that cause the greatest harm.

National Crime Agency (national response)
The NCA targets criminals and groups posing the biggest risks to the UK. In the case of economic crime, its conducts its own operations, providing operational and specialist support to partner agencies and supporting and directing local and regional policing as required.

Regional Fraud Teams (regional response)
Regional fraud teams are embedded within the existing network of Regional Organised Crime Units (ROCUs). For Dorset, this is the Regional Cyber Crime Unit within the South West ROCU – https://www.swrocu.police.uk/cyber-crime/

Police Force Fraud Teams (local response)
Many police forces, not all, have their own dedicated local resources dedicated to tackling economic crime. For Dorset, this is the Dorset Police Economic Crime Unit – https://youtu.be/eKE7yihdlq0 (link to video of DI Andrew Kennard explaining the unit's role).

1.4 Policing has a significantly complex and well-established network to proactively manage fraud and cyber-crime, and therefore the PCC, who continues to support this work, and the victims thereof, has focussed his activity along four main tranches of activity:

- Commissioning and support of policing services;
- Awareness raising;
- Scrutiny of policing activity; and
- National advocacy and campaigning.

2. COMMISSIONING AND SUPPORT OF POLICING SERVICES

2.1 While the specific CyberSafe campaign from the PCC's first term of office has now finished, the PCC-funded appointment of a dedicated Cyber Crime Protect and Prevention Officer (Cyber Protect Officer) has seen a number of initiatives introduced to promote cyber-crime awareness and share crime prevention tools and advice.

2.2 The Cyber Crime section of the Dorset Police website has been developed to incorporate a number of free resources, provide advice and guidance on how to protect against fraud, phishing attacks and sensible tips for effective and secure password management. The website also signposts to further information on a variety of subjects from a range of sources.

2.3 Dorset has a higher than average proportion of older residents, and it is well established that older people are more vulnerable to becoming victims of fraud and cyber-crime. The PCC has therefore, for example, supported the Prama Foundation in funding the purchase of 750 'Scampaks' for distribution to vulnerable older people to raise their awareness of fraud and assist in protecting them against scams.

2.4 The Cyber Protect Officer also continues to work with Dorset Community Action to deliver cyber awareness sessions to older members of the community, and to provide fraud and cyber-crime prevention advice to Dorset Police Neighbourhood Policing Teams for further dissemination to potentially at risk groups.

2.5 A fundamental goal is to drive up the level of reporting, and to help to dispel the stigma around becoming a victim of fraud or cyber-crime. The engagement events, in particular, allow the Cyber Protect Officer to not only help victims and potential victims recognise there is no shame in being caught out by professional fraudsters, who use ever-increasingly sophisticated and plausible methods to commit offences; but also help build confidence within attendees by providing straightforward advice that be taken to help protect their assets.

2.6 Alongside this activity, the regional team also provide a similar service, and have been running a series of online seminars directed at business, focussed around the protection of assets – the details of which can be found here.

2.7 Most recently, in November 2020, the PCC – alongside the other PCCs and Chief Constables across the five-Force South West Police Collaboration Programme – formally agreed to support the funding and development of a regional cyber security resilience centre. Businesses in Dorset now have the opportunity to sign up to the new South West Cyber Resilience Centre, to help better protect them against cyber-crime (www.swcrc.co.uk).

3. AWARENESS RAISING

3.1 Phishing emails, scam phone calls, and malware are just a few ways people can be targeted online and the threat evolves every day. While prevention and awareness-raising activity is key to reducing the number of people affected by fraud, support for those who fall victim is a key concern for the PCC.

3.2 A series of guest blogs on the PCC website have been published to help increase awareness, focusing on topics such as staying safe online, avoiding fraudsters and scammers, the growing threat of romance fraud, and how to avoid Christmas scams.

3.3 The Dorset Police Cyber Protect Officer continues to act as the Force's dedicated resource for advice and guidance to communities. The Cyber Protect Officer uses the Cyber Crime Prevention Toolkit as the basis of which to undertake a number of talks and presentations to businesses and community groups across the county throughout the year – often alongside PCC public engagement events. These sessions are widely advertised through the Dorset Alert messaging service, and the Force's and OPCC's social media accounts, which also provide regular and current updates and advice.

3.4 Most recently, in November 2020, the PCC hosted a well-attended virtual engagement session that focussed on fraud and cyber security. This session was broadcast live, hosted by senior BBC journalist Laurence Herdman, and is available on the PCC's YouTube channel.

4. SCRUTINY OF POLICE ACTIVITY

4.1 In 2017, Dorset Police launched the Banking Protocol, a partnership between the police, finance industry and trading standards. It is a fraud prevention scheme to identify and protect potential fraud victims when they visit a bank or building society, by training bank staff to spot when someone is about to fall victim to a scam and try to prevent them withdrawing cash or transferring money to a fraudster, with an immediate police response to the bank.

4.2 The PCC has also signed up as a Scambassador, part of the National Trading Standards Friends Against Scams initiative, and receives cyber-crime and fraud profiles for Dorset which assist in monitoring issues locally and scrutinising the Force response.

4.3 The business crime strategy developed by the OPCC identifies fraud as a key focus. Businesses have communicated their frustrations to the PCC and Chief Constable on the increased threat from cyber fraud and inconsistencies of safety messages, so this strategy will see the Force work with business leaders to address these concerns.

4.4 The OPCC-led business crime working group is currently leading on the implementation of regular, structured seminars focused around specific topics and issues. It is anticipated that online crimes and fraud will feature significantly within these sessions and provide further opportunities to give tailored crime prevention advice.

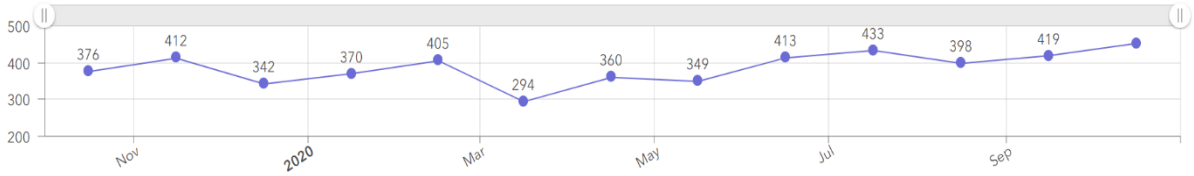
4.5 Most recently, in December 2020, the PCC as part of his national portfolio responsibilities for fraud, made representations to the NPCC leads for Cyber and Economic Crime regarding the local visibility and accountability of fraud offences.

Spotlight: The lack of local fraud data as a barrier to effective PCC scrutiny

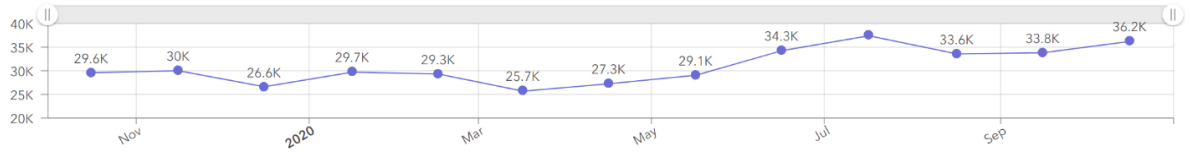
Unlike other notifiable crimes, police forces are required to return data on outcomes resulting from fraud investigations to City of London Police, to aid national reporting to the Home Office. Whilst this centralised process has provided efficiency savings for local Forces, and improved and better standardised recording overall, the downside has been the reduced visibility of local fraud data, making management and scrutiny of local Force performance difficult.

Without regular access to local fraud and cyber-crime data, Chief Constables have been unable to have full understanding about how resources might need to be directed and shifted and PCCs have been unable to effectively scrutinise this area of Force performance.

This position has now been addressed, and the data held by the City of London has been made available to PCCs on a regular basis over the past year, as follows:



The data above are the monthly reporting volumes for fraud and cyber-crime for Dorset, and represent the full extent of data currently available. As stated previously, the data are in line with the national position, which is show below:



5. NATIONAL ADVOCACY AND CAMPAIGNING

5.1 In addition to his local work, the PCC continues to work closely with the City of London Police and National Fraud Investigation Bureau (NFIB) to improve the national fraud reporting position, particularly with regard to victim care and support.

5.2 The PCC has for some years been concerned about the level of service being delivered by Action Fraud, but has been somewhat hamstrung by the lack of evidence, as described in paragraph 4.5. However, he became extremely concerned to read reports in the media about Action Fraud, following an undercover investigation by The Times, whose reporters found evidence that their call handlers were trained to mislead victims into thinking their cases would be investigated when they knew most would never be looked at again.

5.3 The PCC therefore commissioned an OPCC survey to gather his own evidence. This survey, conducted in late 2019, and previously reported to the Panel, found that 71% of respondents who contacted Action Fraud were not happy with how their case was dealt with, whilst 45% stated they did not receive a response after contacting the organisation.

5.4 The survey results and the emerging undercover reporting, allowed the PCC to use his platform to further highlight this unacceptable position, and began to call for an overhaul of the current model by which policing tackles fraud, both publicly, and privately to the national police economic crime lead, as previously highlighted to the Panel.

5.5 Most recently, in September 2020, and as a result of the collective advocacy for the improvement of Action Fraud, it was reported that a new supplier would be found to deliver the Action Fraud service, and that the current supplier would be blocked from delivering any further Government contracts. The PCC continues to work with the City of London Police and National Fraud Investigation Bureau to improve this national capability, particularly with regards to victim care.

6. SUMMARY AND RECOMMENDATION

6.1 Fraud and cyber-crime are complex and demanding areas that require constant vigilance, and the PCC will continue to support the many dedicated officers and staff in Dorset Police who work hard to tackle this ever-growing problem. It is clear however that these crime types are more effectively managed at a national scale.

6.2 The above does not represent an exhaustive list of activity undertaken by the PCC, the Chief Constable, and their partners to address these issues. Of particular note, this report has not highlighted activity undertaken by PCC to strengthen local support available to victims of fraud and cyber-crime, for example.

6.3 Whilst local activity has largely been maintained throughout the PCC's second term, with some escalation during the period of the pandemic, a real change has been brought about on the national scale by the changes around Action Fraud, and it is hoped that the changes that will be enabled by the re-letting of this contract will deliver significant improvements in due course.

6.4 Members are asked to note the report.

SIMON BULLOCK
CHIEF EXECUTIVE

Members' Enquiries to: Simon Bullock, Chief Executive & Monitoring Officer 01202 229084
Media Enquiries to: Susan Bloss, Head of Communications & Engagement
01202 229095