SCOTTISH POLICE AUTHORITY

Agenda Item 6.6

Meeting	**SPA Policing Performance Committee**
Date	**9 March 2021**
Location	**Video Conference**
Title of Paper	**Police Scotland report on Countering Organised Fraud Crime**
Presented By	**T/ACC Patrick Campbell, Organised Crime, CT and Intelligence**
Recommendation to Members	**For Discussion**
Appendix Attached:	**No**

PURPOSE

This report is to provide members with analysis of Serious and Organised Crime Group (SOCG) fraud activity and to explore what measures are being used to gauge effectiveness in this area.

It further provides an overview of approaches being taken to protect, prevent and investigate fraud crimes including cyber-enabled fraud.

Members are invited to discuss the content of this paper.

1. BACKGROUND

1.1 There are 100 SOCGs identified through analysis as being active in Scotland. Of those, 23 SOCGs are identified as being involved in fraud. 87% of SOCGs involved in fraud are linked to businesses that are then used to further criminal activities. SOCGs are using a diverse range of methodologies, with two groups identified as involved in multiple fraud types.

1.2 The most common fraud types used by SOCGs include finance/loan agreements and Business Tax Fraud. Other fraud types include excise duty evasion, high-tech fraud (including vishing – automated voice messaging to a phone), mortgage fraud, benefit fraud, long-firm fraud and rogue trader / bogus crime fraud.

2. TACKLING THE THREAT AND RISK

SOCG's

2.1 Fraud is investigated, disrupted and prevented at all levels within Police Scotland (including local area policing and divisional CID). The role of the Economic Crime and Financial Investigation Unit (ECFIU) relates to countering serious and organised financial crime in Scotland including SOCG's.

2.2 The ECFIU is part of Specialist Crime Division (SCD) with a remit to:

- Investigate major or complex frauds / embezzlements;
- Undertake major enquiries from government departments;
- Investigate commercial crimes against banks and finance houses;
- Investigate fraud, the geographical spread of which makes it impracticable for divisional officers to investigate;
- Assess matters involving public sector corruption, bribery or defalcation.

2.3 Currently the ECFIU are investigating 76 separate instances of reported fraud / financial crime linked to SOCGs amounting to over £70 million.

2.4 Multi-agency investigations and interventions over the last 12 months has seen executive action taken to impact on the SOCG's

involved in serious and organised fraud crimes. This action has allowed for 11 identified SOCG's to have been removed from those seen as presenting a risk owing to their fraudulent activities. Multi-agency efforts continue to reduce the ability of the remaining 23 SOCG's involved in fraudulent crimes to obtain benefit from their criminal activities.

2.5 In conjunction with partners in law enforcement and financial institutions we have used existing processes and legislation to impact on SOCGs' ability to legitimise funds being fraudulently obtained. Since 1 April 2020 to present date, through existing legislation and engagement with COPFS for Confiscation Orders and Civil Recoveries Unit (CRU) for forfeiture of cash and other assets, we have enabled the forfeiture of cash and assets as follows:

Mechanism	Amount
Proceeds of Crime Act (POCA) (year to date figures for POCA represent those provided to COPFS & CRU for consideration of confiscation & forfeiture)	£35,652,308
Confiscations Orders	£ 1,211,813
Civil Recoveries Unit	£ 2,950,955

2.6 These legislative avenues to law enforcement continue to impact on SOCG's ability to gain assets through fraudulent means and Police Scotland, through consultation and liaison with COPFS and CRU, will continue to make use of these mechanisms to impact on SOCGs' ability to benefit from crime.

2.7 In addition to the SOCG impacts of fraud, there continues to be activities which impact on the public whether that be through traditional fraud types or the ever increasing use of cyber-enabled fraud.

2.8 The ECFIU also continue to support the wider approach taken by local policing around the recording and investigation of fraud. This complements Police Scotland's Fraud Action Plan which is administered through the multi-agency approach to fraud taken by the Acquisitive Crime Group.

2.9 An area where Police Scotland, through engagement and collaboration with banking institutions, have had some marked success is through a process jointly developed with the Banking Institutions known as the Banking Protocol. This agreed process allows bank staff dealing with potentially vulnerable members of the public where they suspect that transactions being made at that time are suspicious, can report their concerns to the police and an immediate attendance by police is made at the branch with a view to early intervention. This local level approach has been a huge success and since 1 April 2020 until the most recent data (18 January 2021), there were 703 incidents reported to the police through the Banking Protocol which prevented monies amounting to £3,664,770 being fraudulently obtained.

Partnerships

2.10 Acknowledging that fraud and financial crime are not solely the remit of the Police, it is paramount that we have effective partnerships with other enforcement bodies as well as other organisations across the public and private sectors. Police Scotland work with a large number of partner agencies at a Scottish, UK and International level. It is recognised that in this current digital age and has been brought to the fore recently during the lockdown restrictions, there is an online and cyber aspect to almost all categories of fraud, both targeted at the public and also at businesses and organisations.

2.11 This necessitates the need to increase our understanding of the threats to Scotland from within and out with our own borders. Links with the National Economic Crime Centre (NECC) at a UK National level allows Police Scotland and our partners to better understand the threats and methodologies of crime being perpetrated across the UK and beyond and better align our response whether in an investigative or preventative capacity.

2.12 The Scottish Business Resilience Centre (SBRC) continue to support and work with Police Scotland in looking at new ways to incorporate joined up working between business and the police to better inform, prepare and prevent fraud and cyber-enabled crimes and ensuring that appropriate understanding and reporting channels are identified. This includes recent incidents where Cyber Incident responses have been deployed to organisations where breaches of security to their cyber network have been identified. These incidents

are increasing and through liaison with the SBRC, Police Scotland and wider partners are increasing our capability and capacity to respond to these cyber incidents.

Reporting of fraud

2.13 The recording of crimes and offences provides that in terms of fraud in all of its guises, there has been a marked increase this reporting year when compared against the previous years' data. This increase at the time of this report shows an increase of 38% on last years' fraud figures (2019/20) and is as follows:

Year	2019/20 (full year)	2020/21 (to 21.2.21)
Fraud - recorded crimes	9668	13'339
Detected crimes	3001 (31%)	3115 (23.4%)

2.14 As can be seen, there is also a rise in the overall number of detected cases of fraud this reporting year however, as there has been a sharp rise in reported frauds this year, this reduces the detection rate.

2.15 Whilst effective assessment and analysis of fraud and intelligence will better inform an understanding of the threat that fraud presents, it is widely acknowledged across law enforcement that fraud is a crime that is traditionally under reported. The reach of under reporting spans all aspects of our communities from vulnerable citizens through to multinational companies. The reasons for such under reporting ranges from embarrassment through to commercial implications and the need to protect organisational reputations.

2.16 Recent examples of this include a victim of a particularly prevalent fraud type as this time, referred to as 'romance frauds' where the victims have been befriended, believe that they are in a bona fide relationship which forms usually online, and after a short period is coerced into transferring monies, sometimes very large amounts, to the bank accounts of their perceived 'partner'. The victim, after transferring the monies is then unable to contact their 'partner' and realise they have been the victim of fraud. This type of crime is very personal to the victims and can lead to a reluctance to report.

2.17 These types of frauds have been increasing across the UK during the lockdown periods and campaigns aimed at raising awareness of

these fraud types have been supported by Police Scotland to ensure that persons avoid being the victims of such crimes or where they have been a victim, able to report it and feel supported in doing so.

Communication & prevention

2.18 Focus on disruption and prevention is crucial to counter organised fraud crime. Police Scotland Safer Communities and Corporate Communications ensure appropriate and relevant messaging is communicated to the communities in Scotland to combat the threat through messaging and media campaigns. These campaigns cover a wide variety of frauds and most recently Police Scotland supported the media campaign 'Take Five for Fraud'. This was supported across all Police Scotland media platforms where is realised more than 120'000 visits to the Police Scotland 'Take Five' site. Police Scotland also supported UK national media campaigns in respect of 'Operation Giantkind' – investment fraud and 'Operation Tonic' aimed at romance fraud as mentioned above.

Cyber

2.17 As we move into a more digitally enabled and driven world, the more traditional methods of fraud and financial crime are diminishing with the vast majority of contacts which lead to reported frauds being cyber-enabled. The ability of an individual to perpetrate a crime in Scotland but be physically located anywhere in the world requires that Police Scotland continue to evolve our response and that of our partners and also to develop and maintain strong relationships and working practices across the partners within the UK and internationally.

2.18 Police Scotland's recently published 'Cyber Strategy' and the subsequent implementation of that strategy focusses on 'keeping people safe in the digital world'. One of the key objectives of the strategy is to increase our Cybercrime Investigative capability which will have a positive impact on our visibility and investigative capability online in respect of the investigation of fraud.

2.19 This will be achieved by increasing and aligning our own collective resource in conjunction with developing and strengthening existing links with academia and partners within the public and private sectors with this approach being embedded within the newly formed Centre of Excellence. By adopting this strategy Police Scotland will

strengthen our ability to tackle online fraud from a proactive education and prevention perspective. It will also develop and enhance our reactive, investigative capability and capacity to address the increasing use of complexity and technology to facilitate online criminality.

2.20 Police Scotland will continue to evolve our capabilities and capacity in Cyber Investigations and the Police Scotland commitment to the published Cyber Strategy. Implementation of the strategy will continue to evolve our understanding of the threat of cyber-enabled fraud and options and opportunities to target offenders and better inform the public and partners to prepare, protect and prevent cyber-enabled fraud at all levels.

2.21 The investigation and mitigation of fraud is ever evolving and new methods and ways of working will continue to develop at pace to ensure that Police Scotland and our partners' approach to understanding and tackling fraud remains effective.

3. FINANCIAL IMPLICATIONS

3.1 There are potential financial implications associated with the Cyber Strategy and the evolving increases in cyber-enabled fraud which may require further increases in resource and training to ensure we retain capability and capacity to respond to Cyber incidents.

4. PERSONNEL IMPLICATIONS

4.1 As we further embed the Cyber Strategy and understanding this may lead to an increase in staff engaged in this business area to ensure we have a workforce dedicated to facing the threats identified. This will continue to be reviewed to ensure that any amendments to the operating model in terms of staff engaged in cyber-enabled investigations is understood.

5. LEGAL IMPLICATIONS

5.1 There are potential legal implications in terms of the balance between reported criminal and civil fraud types which is particularly prevalent in respect of frauds reported by business and financial institutions. These need to be managed to ensure that Police Scotland provides a thorough and robust assessment of the different fraud types and mechanisms for conclusion.

6. REPUTATIONAL IMPLICATIONS

6.1 There are potential reputational implications associated with the contents of this paper. Police Scotland will continue to record and investigate fraud and economic crime using traditional investigative techniques and embracing new technology to stay ahead of the perpetrators of this crime type. The ability to utilise and abuse online systems in the preparation and perpetration of these crimes will continue to be a challenge to policing and partners and presents real challenges in terms of the police and partners' ability to keep pace with changes in fraud methodologies and compromises of traditionally safe IT systems such as bank infrastructure.

6.2 Through partnership working and sharing of information Police Scotland will seek to ensure we maintain the ability and technological expertise with which to investigate and support the public, public sector organisations and third sector business partners to identify, mitigate and report fraud and financial crime.

7. SOCIAL IMPLICATIONS

7.1 The continued implementation of the Fraud Action Plan and the Cyber Strategy will provide improvements in the understanding and investigation of SOCG fraud and also wider cyber-enabled fraud in Scotland and provide an enhanced and informed intelligence picture of the prevalence of fraud in communities.

8. COMMUNITY IMPACT

8.1 Continued engagement through established channels around traditional and cyber-enabled fraud trends with the communities and partners will allow for better prevention strategies and also provide opportunities for increases in confidence to report frauds to the police.

9. EQUALITIES IMPLICATIONS

9.1 There are no Equalities implications.

10. ENVIRONMENT IMPLICATIONS

10.1 There are no Environment implications.

RECOMMENDATIONS

Members are invited to discuss the content of this paper.