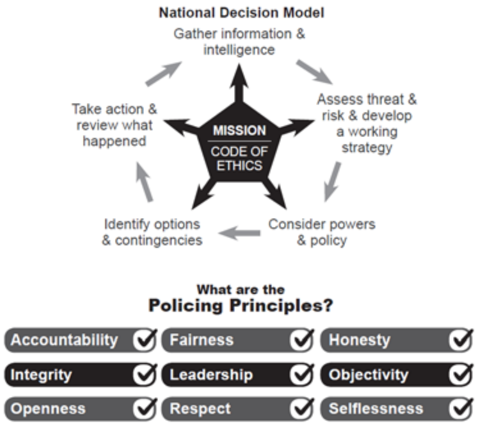
Fraud and Cyber Crime

Required for:	PCC Performance Meeting May 2019
Security Classification:	**Official**
Handling information if required:	n/a
Suitable for publication:	Yes / No
Title:	Fraud & Cyber Crime
Version:	1.0
Purpose:	PCC Performance Meeting May 2019
ACPO / Strategic Lead:	ACC Savell
National Decision Model compliance:	*Yes*
Date created:	1st May 2019
Date to be reviewed:	

AUTHOR:	
Name:	Karen Mizzi
Job Title:	Detective Superintendent
Telephone number:	101


National Decision Model
Gather information & intelligence
Assess threat & risk & develop a working strategy
Consider powers & policy
Identify options & contingencies
Take action & review what happened
MISSION
CODE OF ETHICS
What are the Policing Principles?
Accountability
Fairness
Honesty
Integrity
Leadership
Objectivity
Openness
Respect
Selflessness

1. Background – National context

1.1. Fraud is the most commonly experienced crime in the UK with an annual cost of £190 billion. The most robust figures currently available from the Crime Survey of England and Wales reveal there were 3.4 million incidents of fraud in 2016/17. However it is thought fewer than 20 per cent of incidents of fraud are actually reported so the true figure may be much higher. The true scale of fraud is very significant but also hampers understanding of the threat.

1.2. Cyber Crime continues to rise in scale and complexity, affecting essential services, businesses and private individuals alike and it costs the UK billions of pounds, causes untold damage and threatens national security.

1.3. Economic Crime (Fraud) is a strategic threat and features on the Force control strategy for 2019/2020.

1.4. The most accurate fraud and cyber-crime data is provided by the National Fraud Intelligence Bureau (NFIB). The fraud and cyber-crime profile is published six monthly and is broken down to individual force level. The latest report for Surrey refers to data recovered from April to September 2018 and when applicable is compared to the same reporting period in 2017.

2. Content

2.1. Surrey Police received 2.59 Action Fraud (AF) reports per 1000 residents during the latest reporting period (April to September 2018) compared to 1.79 during the same reporting period in 2017, ranking it 4th in England and Wales; in comparison to census data ranking it 20th in terms of general population size. The most recent data from NFIB indicates that fraud in Surrey increased by 13% from 5,441 (2017) to 6,183 offences over the same period in 2018. This compares to the national increases that sit at around 11%.

2.2. Financial losses in Surrey (April to September 2018) equated to £22.5m compared to £14.5 million during the same period in 2017.

2.3 National statistics indicate that 16% of all fraud is against a vulnerable victim, however, in Surrey this is higher and sits at around 18%. Moreover, 6 out of 20 victims reported that the impact of fraud was severe or significant and this is in line with trends nationally. The most significant victim group identified were those aged between 50-59 years.

2.4 The most common enabler in relation to fraud crime was the telephone (34%); email (13%); online sales (11%). This broadly reflects the national picture.

2.5 The use of charging, cautioning and community resolutions by Surrey Police is noteworthy. There were 207 crime referrals and 110 judicial outcomes. Of these judicial outcomes, 61% resulted in a charge. Additionally, there were 62 crime referrals for intelligence, victim care or other disruption opportunities.

2.6 Nationally, cyber-crime is reported to have increased by 7.9%, however, from April to September 2018, Surrey has seen a greater impact with an increase of 33%, which is 329 cyber dependent crimes during this reporting period, compared to 246 during the same reporting period in 2017 . Total losses in Surrey have reached £2m, which is an increase of 637%, compared to the previous reporting period (October 17 to Mar 18) and compared to a £200k loss during the same period in 2017 (April to September 17), with national losses increasing by only 6%.

2.7 Within Surrey, the most prevalent reported offence is hacking, social media and email. The most significant victim group identified were those aged between 50-59 years.

2.8 Cyber-crime, as opposed to fraud, is more prevalent with individuals rather than business with 80.5% of crime being associated to the person. Furthermore, 224,390 IP addresses used in crime were identified as located within the Surrey

2.9 The joint force Cyber Crime unit has been fully collaborated since its inception in 2015. This small team provide investigative provision for all cyber dependent crimes received across Surrey and Sussex, providing tactical advice in respect of cyber enabled crime and subject matter expertise around the digital aspect of investigations. The team recently received an uplift in resource, through national transformation funding of 1 x Detective Constable and 1 x Cyber Protect officer.

3 HMICFRS Report on Fraud Published April 2019 – Force Performance

3.1 Surrey Police NPCC strategic lead for fraud is ACC Savell (Specialist Crime Command) with overarching responsibility for the recommendations and Areas for Improvement (AFI) outlined in the HMICFRS report.

3.2 The below is a brief overview of the Surrey Police position in relation to these recommendations / AFI's.

3.3 **Recommendation – By March 2020, the NPCC Coordinator for Economic Crime and Chief Constables should ensure that forces have processes in place to accurately and efficiently report Fraud outcomes to the National Fraud Intelligence Bureau.**

The force recognises that there is a gap and is taking steps to work with the NPCC Coordinator for Economic Crime to ensure the necessary processes are in place to ensure fraud outcomes are accurately recorded and shared with the NFIB by March 2020 and this work has been allocated to the Fraud Working Group for development.

3.4 **Recommendation – By September 2019, Chief Constables should publish their force's policy for responding to and investigating allegations of fraud (in relation to both calls for service and National Fraud Intelligence Bureau disseminations for enforcement).**

At the time of publication of this document there is currently no national Fraud Strategy in place or force level. We are working with the National Coordinator for Economic Crime to ensure the force strategy is published by September 2019.

3.5 **Area for Improvement** - **the way the force uses the National Fraud Intelligence Bureau (NFIB) monthly victim lists to identify and support vulnerable victims and others who require additional support**

Surrey Police already has a process in place to identify vulnerable victims of fraud and the process is as follows:

- *NFIB fraud victim data is received into the Force by the Action Fraud (AF) SPoC,*
- *The data is sent to the Force Intelligence Bureau (FIB) and is 'washed' against a set list of words that links to victim vulnerability,*
- *Vulnerably list is returned to the AF SPoC,*
- *AF SPoC raises a (CAD) tasking for a Neighbour Officer to visit the vulnerable victim,*
- *After the visit if there are any UK based Lines of Enquiry then it is allocated to Investigations but if there are none, then the report is filed as No Further Action*
- *In either case the victim is assessed to see whether any prevention / safeguarding measures need to be put in place (including telephone call blockers), and*
- *Surrey is developing a business case to employ a Victim Support Fraud Caseworker who will focus on the Medium / High risk victims (taken from the SCARF risk assessment) that ensures they are visited and support is given.*

The Economic Crime Unit is piloting a Volunteer Fraud Prevention Project on West Sussex Division aimed at non vulnerable victims and businesses with a data washing process to identify which "package" of protect support they will receive. Once the concept has been proven it will be rolled out to all divisions across Surrey & Sussex.

3.6 **Ensure the force improve the identification and mapping of organised crime groups in which the principal criminality is fraud**

The force TTCG OCG mapping process assists the force to identify and assess the threat posed by Organised Crime Groups (OCG's). Fraud OCG's at force level are being mapped and scored (where appropriate), using thematic MoRiLE and the OCGM mapping tool. However it is recognised that this is an area which the force can improve upon at divisional / departmental level and is an action for the force fraud working group to address.

3.7 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

Surrey Police maximises the use of all its available powers and partnerships (NCA / SEROCU Asset Recovery Team/ Trading Standards) to prevent offender's continuing to offend. There is an established prevent approach with the Banking sector titled ' Banking Protocol', increased use of Bank Account freezing orders, = Proceeds of Crime Act (POCA) legislation and Suspicious Activity Reports (SARs) intelligence reports. There is an opportunity to further develop the force approach to prevent tactics through a whole system response to maximise use of POCA legislation and is being progressed through the force fraud working group to progress. Fraud features as one of the Surrey SOC Partnership Board's work streams for 2019/20. There are currently no Fraud subjects currently under the IOM process across Surrey Police area.

3.8 Increase the force's use of ancillary orders against fraudsters

The force has a number of ancillary order options available to it to prevent offenders from continuing to commit fraud and that includes the use of Serious Crime Prevention Orders (SCPO's). We currently have an application pending with the court for an SCPO's against an OCG involved in Fraud. The force also uses forfeiture and confiscation legislation both under POCA and PACE (see table below).

Surrey Police refer Consent Suspicious Activity Reports (SARS) to the Regional Asset Recovery Team (RART) to consider Account Freezing Orders under the Operation Climate agreement. As such we can show we are not only considering them but also using these powers.

The below tables sets out current performance for Surrey for the last twelve months:

	Surrey
Cash seizures under Sec 294 POCA Number	88
Cash seizures under Sec 294 POCA Value	£517,835.48
Section 298 Forfeiture number	31
Section 298 Forfeiture orders	£355,563.52
Confiscation orders obtained	£2,392,877.23
Restraint orders obtained	4
SARS – Number disseminated	6933
SARS - Number of reviewed	3,426
Number of SARs developed	72
DAML's received	55
DAML's refused	None
Confiscation uplifts	£212,037.04

3.9 Ensure that the force complies with the Code of Practice for Victims of Crime when investigating fraud.

Investigators are required under the Victims Code of Practice to keep victims of crime informed of progress of their investigation. Fraud Victim data is not specifically monitored due to the various processes of how victims are supported. This AFI has been referred to the force lead for victim contact and engagement to examine the various streams and to oversee the development of a process that monitors the contact with fraud victims.

4 Conclusion[s]

4.1 As a Force, Surrey is currently well placed to meet the requirements outlined in the HMICFRS Fraud report recommendations and will continue to develop a partnership approach to manage the demands and challenges it faces from the impact of Fraud and Cyber Crime on policing.

5 Decision[s] Required

5.1 None, this paper is for information only