# Fraud and cyber crime

| | |
|---|---|
| **Required for:** | PCC Performance meeting, 22 March 2018 |
| **Security Classification:** | **OFFICIAL** |
| **Handling information if required:** | |
| **Suitable for publication:** | *Yes* |
| **Title:** | Fraud and cyber-crime – position paper |
| **Version:** | v1 |
| **Purpose:** | Briefing on force position on fraud and cyber-crime |
| **ACPO / Strategic Lead:** | ACC Jeremy Burton |
| **National Decision Model compliance:** | *Yes* |
| **Date created:** | 28/02/18 |
| **Date to be reviewed:** | |



| | |
|---|---|
| **AUTHOR:** | |
| **Name:** | Mark Chapman |
| **Job Title:** | Detective Chief Inspector |
| **Telephone number:** | 101 |
| **Email address:** | Mark.chapman@surrey.pnn.police.uk |




## 1. Background

**1.1.** This report outlines the Surrey Police position in respect of fraud and cyber-crime. The report provides local context to the threat posed by these crime types and the local response to these themes.

**1.2.** This paper also covers Surrey Police plans to tackle fraud and cyber-crime in context of national increase, resource implications, and national initiatives.

## 2. Content

### Fraud

### Profile

**2.1.** The NFIB fraud profile for Surrey (April 2017- October 2017) demonstrates there has been a rise in fraud offences compared to the previous reporting period. This is in line with national total volume. Victim losses were estimated at £14.5 million. The most frequently reported fraud types within Surrey were Cheque, Plastic Card and Online Bank Accounts (1,854 reports), Application Fraud (769 reports) and Telecom Industry Fraud (405 reports). Six out of twenty victims reported a severe or significant impact from the crime.

**2.2.** During this time period 440 crime referrals were received by Surrey Police, with 84 judicial outcomes recorded.

**2.3.** The profile indicates that the most common enablers of fraud offences were telephone (31%), online sales (15%), and email (13%), therefore indicating the prevalence of cyber enabled fraud offending.

**2.4.** When considering Action Fraud reports per 1000 population, Surrey Police force area received approximately 1.86 reports per 1,000 residents, ranking it 4th in England and Wales. In comparison, census data ranks it 20th in terms of general population size. The Surrey force area received a higher number of reports per 1,000 residents than other South East region forces (Thames Valley 1.77, Sussex 1.76 and Kent 1.71).

**2.5.** As of September 2017 there were 39 mapped OCGs engaged in Economic Crime (amongst other criminality types) that impacted upon Surrey Police area.

### Response

**2.6.** Surrey Police have established a fraud working group chaired by DCI Chapman to provide a cross force response to the threat posed by fraud offences. This group have developed an action plan based on the 4P framework of Pursue, Prevent, Protect and Prepare. Example work stream areas are the development of officer awareness of fraud offences, implementation and development of Op Signature, development of a communications strategy, training, and the allocation of fraud investigations

**2.7.** The group is committed to providing support and guidance to divisional officers, many of whom may not have the experience or expertise to effectively respond to fraud offences. The majority of fraud offences sit with APT investigators who may not have been provided with training or guidance around this crime type since the change in policing model. There is obvious overlap with the Volume Crime Investigation Improvement Plan capability strand.

**2.8.** The training support also extends into the contact teams where there is particular onus on teams to correctly identify fraud offences and if there is a call for service at the point of report.

**2.9.** The force has invited City of London Police to complete a three day inspection capability and process around fraud investigation.

**2.10.** The force continues to implement Operation Signature which identifies opportunities to safeguard and prevent vulnerable victims from becoming repeat victims. In addition to all recorded fraud offences in Surrey, the Action Fraud co-ordinator proactively scans ICAD's and other crime reports for the indicators of fraud. Each division has Op Signature SPOC's with the safeguarding support being delivered through Neighbourhood teams.

**2.11.** In October 2017, in partnership with Financial Fraud Action UK, Surrey Police established the Banking Protocol which aims to provide an immediate Police response to instances where bank staff feel that vulnerable victims are being pressured into making large payments to a third party.

This immediate response will be to safeguard the vulnerable, secure and preserve evidence of offences, and to effect arrest where appropriate. Since the launch of the protocol over £168,000 has been prevented from being lost by victims and has directly resulted in an arrest.

**2.12.** The Specialist Crime Change Programme proposes changes in the response to specialist fraud investigations within ECU in that the establishment will change from four DC posts and two specialist fraud investigator posts (police staff), to five DC posts. This change will allow for greater flex across the command.

**2.13.** Surrey Police back the UK Finance campaign 'Take Five' which encourages the public to take five minutes to consider sharing payment or personal details when asked. This message is simple and effective in preventing offences.

**Cyber**

**Profile**

**2.14.** The NFIB cyber profile for Surrey (April 2017- October 2017) focuses solely on cyber dependant crime with this product being the first of its type received by the force. This report demonstrates there has been a reduction in identified offences of 12.5% to 246 offences within this reporting period. The total financial loss was £200k. The most prominent offences were through the introduction of computer viruses, malware, and spyware onto devices. Of interest is the fact that 94.3% of reports were received from individual victims, indicating a reluctance of business to report cyber intrusions.

**2.15.** As a new product from NFIB, this report is based upon relatively low data sets, and tends to concentrate on events that have been experienced nationally. This product will evolve to become more informative as it develops. This report does not seek to provide the description around different types of cyber-attack that is contained within the report.

**Response**

**2.16.** The response to cyber dependant crime is provided via the joint Surrey and Sussex Cyber-Crime unit (CCU). CCU support the investigation and disruption of serious crime, harm and risk through covert and overt support to both forces. The CCU investigate offences under the Computer Misuse Act, and have oversight of digital media investigators (DMI) who advise on Cyber enabled crime investigations and lower risk operations on divisions.

**2.17.** The CCU work to a strategic delivery plan based on the 4P framework of Pursue, Prevent, Protect, Prepare. This work reports into the Digital Investigations and Intelligence Oversight Board, through which a joint force action plan is managed.

**2.18.** Example workstream areas are the assessment of young people who have been drawn into cybercrime offending for their suitability for the Cyber Security Challenge – a national diversion scheme run in conjunction with the NCA under Prevent. The CCU work with partners in the public and private sector, businesses and academia to promote Cyber Security to the people who live and work in Surrey and Sussex to enable them to protect themselves against online threats and vulnerabilities under Protect.

**2.19.** The CCU are currently out of scope of the Specialist Crime Change programme, with the consideration of a regional response to cyber dependant crime being managed under South East Regional Integration Programme (SERIP).

**2.20.** Surrey Police would like to encourage the business community to engage and report offences. Additionally, simple prevention advice is for business and personal users to maintain up to date virus protection.

**2.21.** The Surrey & Sussex CCU is currently engaged in a national exercise to test the aggregated response to a large scale cyber-attack.

## 3. Decision[s] Required

**3.1.** This paper is for information only.

## 4. Background Papers

**4.1.** NFIB Fraud profile for Surrey April 2017- October 2017 (available on request)

**4.2.** NFIB Cyber profile for Surrey April 2017- October 2017 (available on request)