Online Crime Evidence

Contents Page

Project FALCON Implementation team - October 2014

London Assembly report - Project FALCON.

Summary

This paper provides a response to a request for further information on FALCON originating from representatives of the London Assembly.

The request for further information is listed at part A of this document. Part B outlines the response.

Request for further information following meeting with Detective Superintendent Jayne Snelgrove, 5 August 2014

1. Please provide the paper you mentioned that has definitions of the different categories of cyber-crime with some examples of the high volume crimes in each category.

1.1 The adopted definition of Cyber Crime is:

1. Cyber Dependent Crimes, where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to commit further crime).
2. Cyber Enabled Crimes. 'Existing' crimes that have been transformed in scale or form by their use of the Internet. The growth of the Internet has allowed these crimes to be carried out on an industrial scale.
3. The use of the Internet to facilitate drug dealing, people smuggling and many other 'traditional' crime types.

1.2 Examples of high volume crimes in each category are as follows:

1. Malware attacks, some forms of phishing, hacking.
2. Frauds including (but not limited to) online and retail fraud, dating scams, ponzi and pyramid schemes, ticket scams, investment fraud and credit card fraud.
3. Harassment, domestic violence related offences, terrorism & related activities.

2. Please provide the FALCON overview/strategy paper you mentioned when it is finalized.

2.1 Please see Appendix 2.

3. Please review the FALCON organisational diagram.

3.1 Please see Appendix 1 for an accurate organisational diagram.

4. For each of the units within the FALCON command, please provide the proposed annual revenue budget at phase 3 (£22 million pa in total), including how much is funded via Home Office contributions as well as staffing resources, broken down between Full Time Equivalents (FTEs) for police staff and police officers (392 FTEs in total).

4.1 FALCON has not yet achieved phase 3. However, please see below breakdown of staff allocation if phase 3 (as per design) is met.

4.2 Current resource and staff allocation within FALCON (building towards **phase 2**) aims to establish a strength of 303 posts (not including management above DCI).

4.3 Column 1 shows the staff allocation before FALCON (but after the transfer of function to the NCA).

	Prior to FALCON	**Phase 2**	**Phase 3**
	Total FTE	**Total FTE**	**Total FTE**
Det Ch Insp	2	3	3
Det Insp	4	9	9
Det Sgt	13	30	40
Det Const	79	207	241
Band C	2	3	21
Band N	3	6	6
Band D	3	23	46
Band E	7	21	24
Band F	1	1	1
Total	**114**	**303**	**391**
Approx Resource	£6.5 million	£17.1 million	£21.3 million

5. Please also provide, where applicable, the equivalent details – annual revenue budget and staffing resources – for each unit prior to the creation of the FALCON command, but following the transfer of functions to the National Crime Agency, to enable a comparison.

5.1 Please see column 1 at 4.3 (above).

6. Please provide a brief description of how typical cyber-frauds are processed in the MPS's crime reporting system (i.e. no crimed) and why this means some outcomes may not be reported back to Action Fraud. If possible, please provide a report that shows the number of 'no crimed' cyber-enabled offences that the MPS recorded in 2011-12, 2012-13 and 2013-14.

6.1 All frauds reported to the MPS, whether directly by the public (in case of emergency) or via Action Fraud (AF) are counted as "no crimes". This is because Action Fraud is the national reporting centre for cyber crime and fraud. AF counts these crimes for Home Office purposes.

6.2 AF/ NFIB assess all crimes reported to them. Each individual victim generates a NFRC number.

6.3 Those which are assessed to have viable leads are then passed to forces to investigate.

6.4 In the MPS, a suspect may be arrested and charged for a relevant offence. In this case the outcome should be reported back to AF.

6.5 However, not all outcomes reported back to AF (or NFIB) have been captured. Some limitations of current IT systems do not permit this to be captured meaningfully.

6.6 Attached below is the data requested from Feb 2013, when this reporting system was introduced. Prior to this the MPS counted frauds in a different manner.

6.7 Please also note, each AF NRFC number pertains to one victim. MPS systems do not count the number of victims in the same manner. MPS systems capture the number of 'cases' (a linked series of offences with 200+ victims will count as 1 report for the MPS, but 200+ reports for AF).

6.8 The table below refers to MPS cases. For the reason described at 6.7, this is likely to be fewer than any corresponding AF figures.

Count of Offences for Non Crime Action Fraud (999/53) & Non Crime Action Fraud Cyber Crime (999/54)
Recorded in the period 1st February 2013 - 31st August 2014

		Non Crime Action Fraud & Cyber crime		
Year	**Month**	**Offences**	**Offences Cleared Up**	**% Offences Cleared Up**
2013	Feb*	966	150	15.5%
	Mar	1014	156	15.4%
2013	Apr*	1135	185	16.3%
	May	1102	199	18.1%
	Jun	1019	185	18.2%
	Jul	1238	158	12.8%
	Aug	1279	201	15.7%
	Sep	1306	169	12.9%
	Oct	1495	192	12.8%
	Nov	1537	180	11.7%
	Dec	1393	185	13.3%
2014	Jan	1396	195	14.0%
	Feb	1299	137	10.5%
	Mar	1519	163	10.7%
FY 13/14 Total		**15718**	**2149**	**13.7%**
2014	Apr	1311	153	11.7%

	May	1348	110	8.2%
	Jun	1413	99	7.0%
	Jul	1486	108	7.3%
	Aug	1445	79	5.5%
FYTD 2014/15 Total So far		**6878**	**548**	**8.0%**
Grand Total		**24365**	**2994**	**12.3%**

Notes

The data in this report was extracted from the live CRIS MIS system on 23rd September 2014.
Live data is subject to change as records are reviewed and updated.

The following Home Office codes were used

999/53	Non-crime fraud - Action Fraud
999/54	Non-crime cyber crime - Action Fraud

Please note that 999/53 was only officially introduced from February 2013, and 999/54 was only officially introduced from the middle of April 2013.

Both of these home office codes (999/53 and 999/54) are non notifiable to the Home Office. Therefore there could be some undercounting as non notifiable offences are not always required to be recorded on MPS systems.

Note with regards to Offences that have been Cleared Up

Please note that the Offences Cleared Up counts are based on the Class Cleared Up Reason field in CRIS. If this field is not null or blank then that offence has been determined as having been cleared up. This includes such clear ups as Restorative Justice and Community Resolutions and not just official Sanction Detections.

7. Please confirm whether or not the MPS has a 'cyber-enabled' flag on its crime reporting system that can be checked when an officer enters a crime report. If so, please provide a report that shows the number of crimes flagged as cyber-enabled that the MPS recorded in 2011-12, 2012-13 and 2013-14.

7.1 The MPS does not use a 'cyber-enabled' flag.

7.2 It uses two features codes (MZ and MY)* which indicate cyber elements to an offence.

7.3 However, these feature codes are not mandatory requirements for crime reporting. They are used to highlight special features or methodologies for analytical purposes.

7.4 Below is a table which shows the use of these codes. Please note, in 2013/2014, the significant drop in numbers is due to the national cyber and fraud reporting centre (Action Fraud) taking on responsibility for reports.

7.5 2014/2015 figures are for part a year and should not be used for comparison.

*MY - Computer is target of the offence (offences under s1 -3 Computer Misuse Act 1990

MZ - Sec 1 Malicious Communications Act, Blackmail, online banking and auction frauds, advance fee frauds and cyberlaundering offences

Total Notifiable Offences flagged with either MZ or MY. Recorded between the 1st April 2011 and 30th September 2014

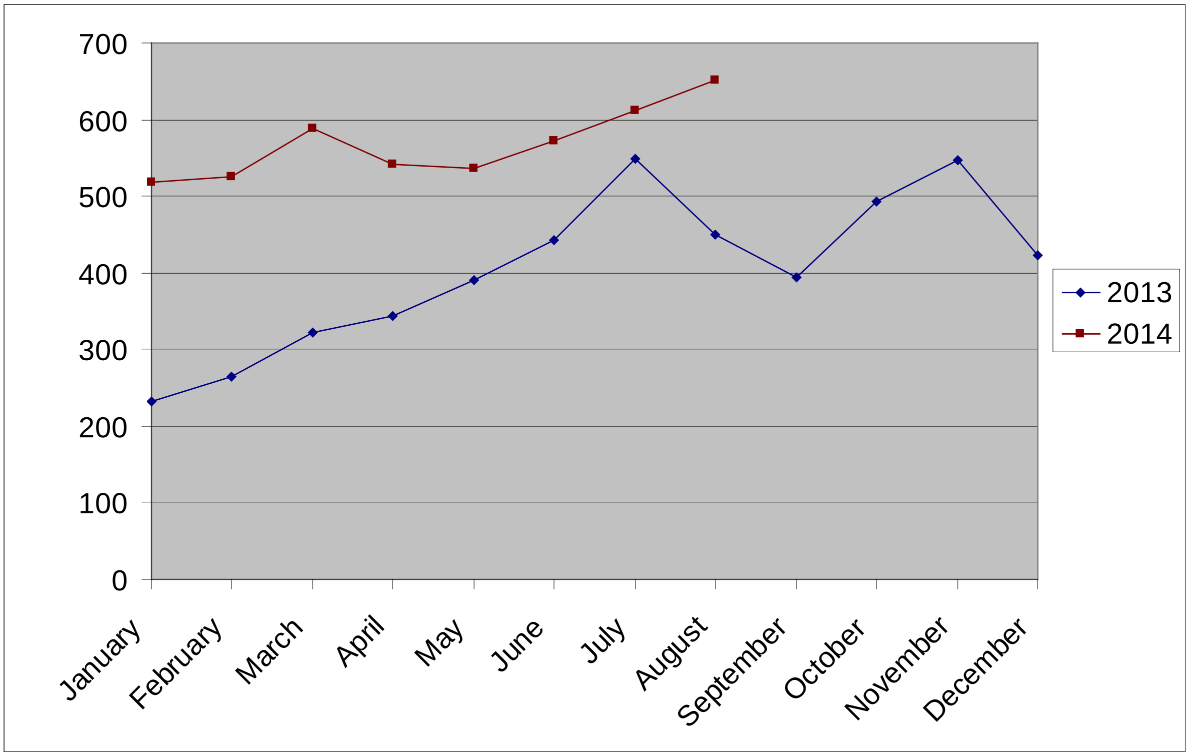
		Financial Year			
Major Class Description	**Minor Class Description**	**2011/12**	**2012/13**	**2013/14**	**2014/15***
Violence Against The Person	Assault With Injury Common Assault Harassment Other Violence	0 1 56 1	1 1 112 1	0 6 135 1	0 1 40 0
Violence Against The Person Total		***58***	***115***	***142***	***41***
Sexual Offences Total		***2***	***0***	***3***	***4***
Robbery	Personal Property	1	0	1	0
Robbery Total		***1***	***0***	***1***	***0***
Burglary	Burglary In A Dwelling Burglary In Other Buildings	0 0	1 3	1 5	1 0
Burglary Total		***0***	***4***	***6***	***1***
Theft & Handling	Other Theft Handling Stolen Goods Theft Person	11 0 0	10 1 0	10 1 1	1 0 0
Theft & Handling Total		***11***	***11***	***12***	***1***
Fraud & Forgery	Counted Per Victim Other Fraud & Forgery	624 298	1161 285	0 1	0 0
Fraud & Forgery Total		***922***	***1446***	***1***	***0***
Criminal Damage	Criminal Damage To Other Building Other Criminal Damage	0 1	0 3	1 3	0 2
Criminal Damage Total		***1***	***3***	***4***	***2***
Drugs	Possession Of Drugs	0	1	0	0
Drugs Total		***0***	***1***	***0***	***0***
Other Notifiable Offences	Other Notifiable	25	27	50	19
Other Notifiable Offences Total		***25***	***27***	***50***	***19***
Grand Total		**1020**	**1607**	**219**	**68**

8. An MPS briefing note on cyber-crime says that Project FALCON is being developed to 'respond to the significant growth in cyber-enabled acquisitive crime'. If requests 6 and 7 above are not possible or do not show this growth, does the MPS have any other data that we can have to support this statement? (I.e. other statistics showing an increase in cyber-enabled acquisitive crime in recent years)

8.1 The above table at 6 is indicative of the rise in cyber and cyber-enabled offences such as fraud. It shows comparative growth within the MPS of such crimes, notwithstanding the issues around recording and reporting of such crimes.

8.2 The below table also shows the growth in MPS crime reports generated from AF referrals.

	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec
2013	233	265	322	344	391	443	548	449	394	493	547	422
2014	518	525	589	542	537	572	612	651				



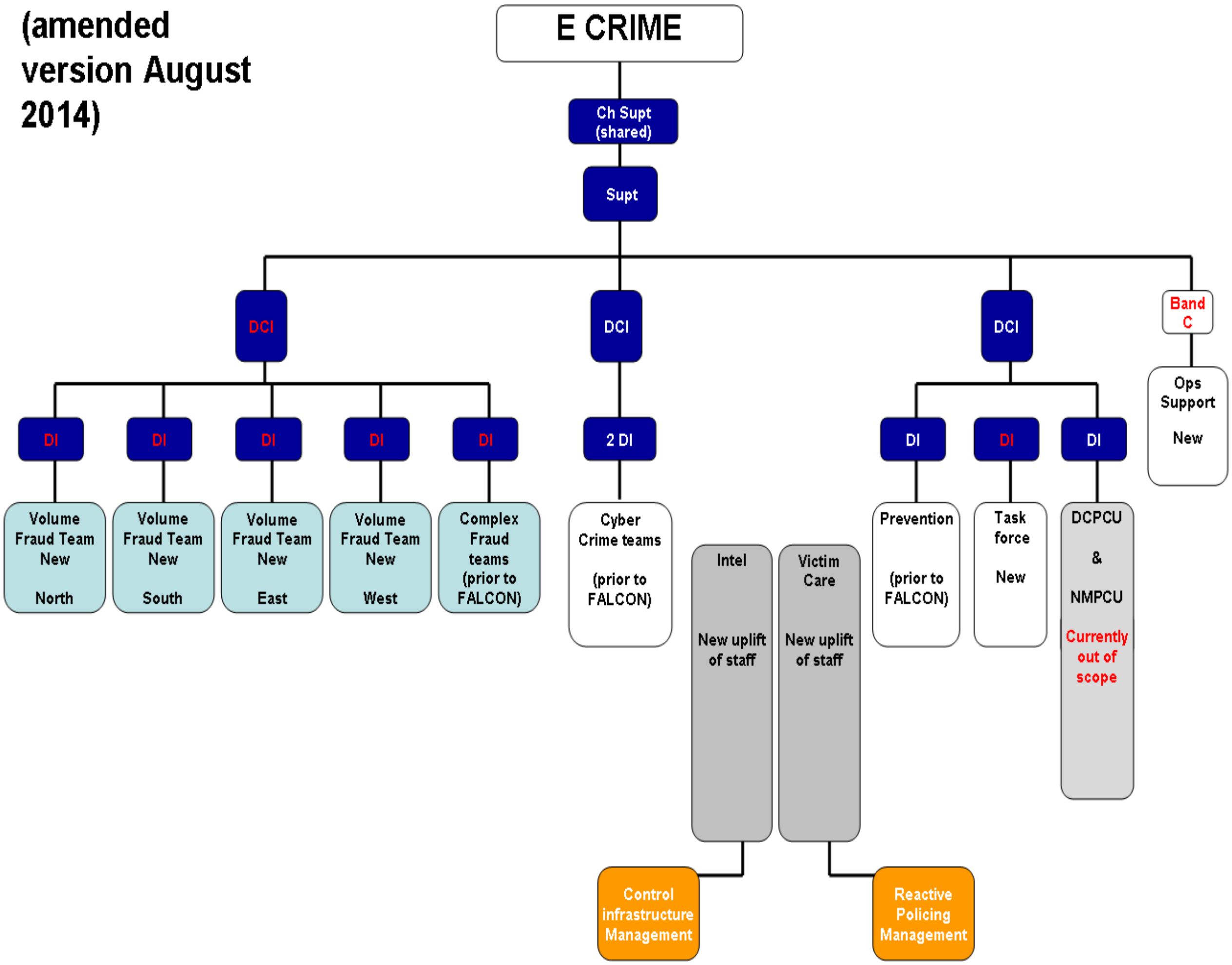
8.3 However, there are a number of reasons to believe this crime is under-reported including:

- Data from the British Crime Survey
- Evidence that victims of fraud are too embarrassed to report (e.g., victims of dating or phishing scams; businesses not wishing to suffer reputational damage).
- Crimes under-reported as the victim does not feel the police or any other agency can do anything about it
- Crimes under-reported because the victim has been recompensed for any losses by their credit card company / financial institution or bank
- Crimes under-reported because neither the victim nor the police recognise that an offence has occurred
- Crimes reported to non-police agencies (e.g., banks or service providers, online retailers etc) which are not notified to police
- Direct evidence from London-based businesses that cyber and online fraud are massively under-reported as they manage incidents themselves and have little confidence in the policing response or reporting mechanisms

- Additionally, data from the Office of National Statistics also shows a rise of 17% in reported fraud offences year on year (192% since 2008/09). Copy this link into your browser for further: http://www.ons.gov.uk/ons/dcp171778_371127.pdf

Appendix 1

Phase 2 (amended version August 2014)


E CRIME
Ch Supt (shared)
Supt
DCI
DCI
DCI
Band C
Ops Support New
DI
DI
DI
DI
DI
2 DI
DI
DI
DI
Volume Fraud Team New North
Volume Fraud Team New South
Volume Fraud Team New East
Volume Fraud Team New West
Complex Fraud teams (prior to FALCON)
Cyber Crime teams (prior to FALCON)
Intel New uplift of staff
Victim Care New uplift of staff
Prevention (prior to FALCON)
Task force New
DCPCU & NMPCU Currently out of scope
Control infrastructure Management
Reactive Policing Management

Appendix 2 - FALCON Objectives and Performance

Our mission: To reduce the harm caused by fraud and cyber criminals in London.

FALCON will:

- **Effective response** - Ensure all Action Fraud (AF) referrals to the MPS are effectively responded by dedicated fraud / cyber investigators
- **Excellent Service** - Provide excellent victim care and seek compensation for our victims wherever possible
- **More justice** - Significantly increase the numbers of arrests and charges relating to fraud and cyber crime
- **Reduce harm** - Proactively target cyber criminals and fraudsters, focusing on stemming the harm caused by the most prolific Organised Crime Groups
- **Better Service for Businesses** - Work in partnership with businesses to improve our response to fraud and cyber crime affecting London's businesses
- **Proactive Prevention** - Undertake targeted prevention work with industry partners that designs out crime, tackles the enablers of cyber crime & fraud and raises the awareness within the public and businesses

We are committed to improving in all areas:

- **Effective Response** - An outcome rate for Action Fraud Referrals - 50% (35% for 14/15)
- **Excellent Service** – Improving victim satisfaction and seeking compensation / repatriation of victim's money more often (no baseline)
- **More Justice** - A four fold increase in fraud and cyber crime arrests and charges
- **Reduce Harm** – Double the number of Organised Crime Groups disrupted
- **Better Service for Businesses** - Increase Business Satisfaction (MOPAC Business Attitude Survey)
- **Proactive Prevention** – Reduce the harm caused by the most prevalent fraud and cyber crimes through prevention action (requires financial harm reduction measures)

What we will measure to ensure we are reaching our goals (Internal use):

- Number of disseminations accepted from Action Fraud
- Number of outcomes in response to Action Fraud referrals
- Number of quantifiable interventions against fraudulent activity (we need to define what an intervention in this area looks like).
- Value of assets seized/disrupted (£m) as a result of quantifiable interventions against fraudulent activity
- Number (of victims for which) and amount of compensation awarded to victims

- Amount of assets / money obtained through fraud & cyber restrained and prevented from loss
- Number of proactive prevention/enforcement initiatives against business crime
- Number of individuals arrested for fraud & cyber crime offences
- Number of individuals charged with fraud & cyber crime offences
- SD rate for fraud & cyber crime (to be best in most similar force grouping. This consists of MPS, West Midlands, Greater Manchester & West Yorkshire).
- Business satisfaction through MOPAC survey

NB: the majority but not all of these will feature in the 14/15 SCO score card. The first performance report will be provided to Crime Fighters in December 2014.

Appendix 3 - Fraud reporting flowchart and contextual information

Action Fraud
flowchart.pdf

A4. Reporting fraud and counting fraud.

All fraud & cyber crime is reported direct to the national fraud and cyber reporting centre, Action Fraud, apart from when the following general conditions apply.

A4.1 Calls to service and vulnerable victims.

A4.1.1 The criteria for a call to service are outlined in the attached pdf document. If these criteria apply, or the victim is vulnerable, then MPS officers attend. MPS officers will report the crime and inform Action Fraud (or assist the victim in reporting the crime to Action Fraud). MPS officers initiate an investigation where appropriate to do so.

A4.1.2 Generally, in all other instances the informant or victim is referred to Action fraud to report their information or crime.

A4.2 Report handling and counting

A4.2.1 Action Fraud collate all reports, whether from police, directly from victims or industry. These are then assessed both by automated means and by crime reviewers (National Fraud Intelligence Bureau, NFIB) to determine those with viable lines of enquiry.

A4.2.2 Each victim captured by Action Fraud is provided with an NFRC number.

A4.2.3 Action Fraud capture the crimes for Home Office counting purposes. Hence any disseminations to police forces are not additionally counted as crimes by those police forces, to prevent duplication (i.e., to prevent the same crime being counted twice).

A4.2.4 NFRC numbers with a viable lead are disseminated to police forces to investigate.

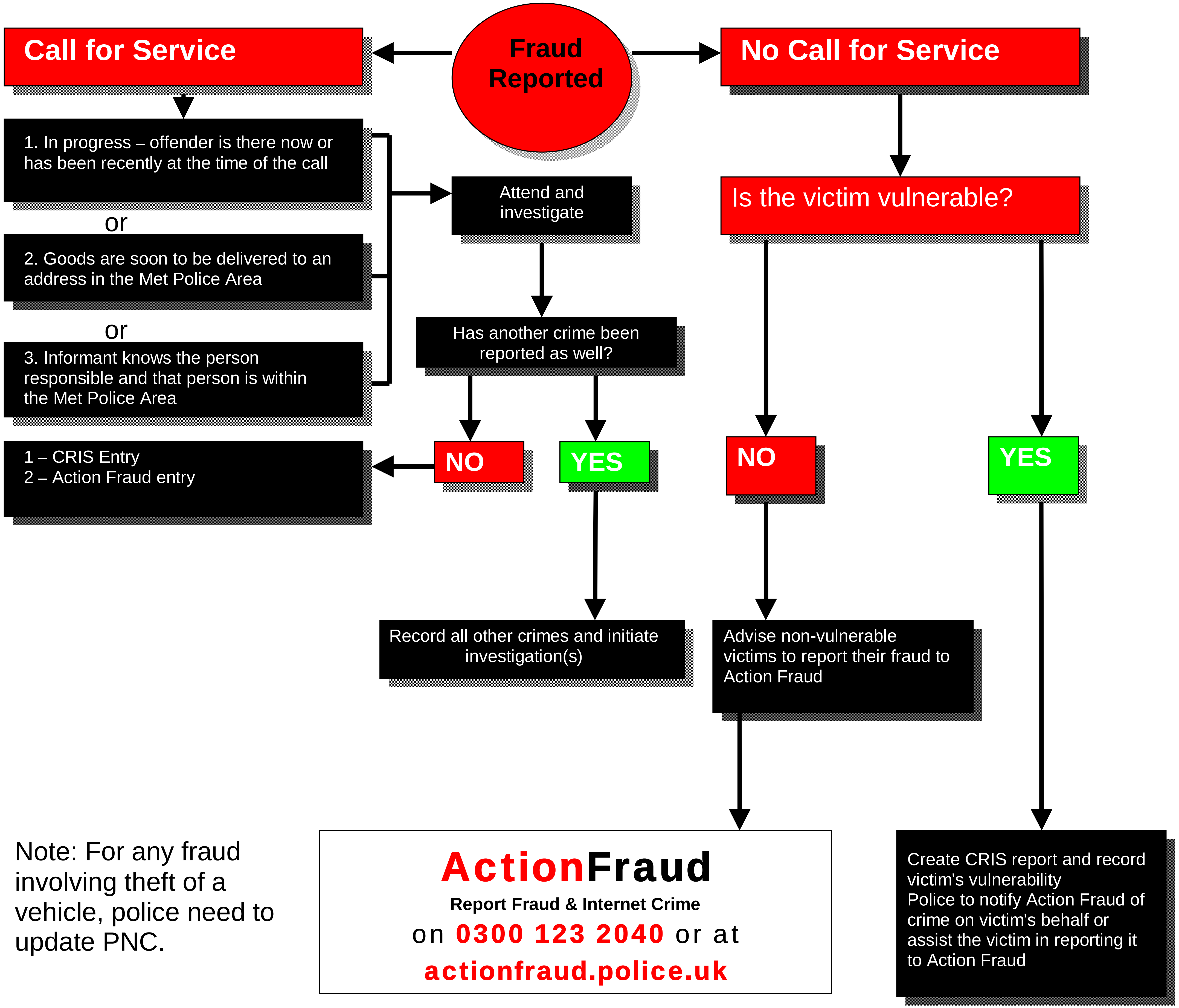
A4.2.5 Police officers investigate the disseminated reports to achieve an outcome.

A4.2.6 Outcomes are reported back to Action Fraud (via the NFIB).

A4.2.7 MPS case management and crime recording systems do not capture all NFRC disseminations as separate reports. A linked series of offences (multiple victims & hence multiple NFRC numbers) can be captured in one MPS crime report (CRiS) for investigative purposes.

A4.2.8 This means MPS records are lower than the numbers of disseminations made by Action Fraud.

A4.2.9 MPS and AF / NFIB IT systems are not interoperable at this time, meaning all disseminations / referrals and related outcomes must be manually keyed between agencies.



Fraud Reported

Call for Service

1. In progress – offender is there now or has been recently at the time of the call

or

2. Goods are soon to be delivered to an address in the Met Police Area

or

3. Informant knows the person responsible and that person is within the Met Police Area

Attend and investigate

Has another crime been reported as well?

NO

1 – CRIS Entry
2 – Action Fraud entry

YES

Record all other crimes and initiate investigation(s)

No Call for Service

Is the victim vulnerable?

NO

Advise non-vulnerable victims to report their fraud to Action Fraud

ActionFraud

Report Fraud & Internet Crime

on **0300 123 2040** or at

actionfraud.police.uk

YES

Create CRIS report and record victim's vulnerability
Police to notify Action Fraud of crime on victim's behalf or assist the victim in reporting it to Action Fraud

Note: For any fraud involving theft of a vehicle, police need to update PNC.

Offences that must be crimed - all others should be reported to Action Fraud:

- Making or supplying article(s) for use in fraud
- Possess/control article(s) for use in fraud
- Possession of false documents
- Making off without payment (including all forms of bilking)
- Theft of fuel
- Forgery or use of drug prescription
- Forgery, etc., associated with vehicle or driver records
- Other forgery

EVEN IF AN OFFENCE IS REFERRED TO ACTION FRAUD, CONSIDERATION SHOULD BE GIVEN TO SEIZING ANY AVAILABLE MATERIAL (CCTV etc.)

Note: For any fraud involving theft of a vehicle, police need to update PNC

FALCON
FRAUD AND LINKED CRIME ONLINE

Room 593
New Scotland Yard
Broadway
London SW1H 0BG

Date: 24 December 2014

Mr Roger Evans AM
London Assembly

(Via email)

Dear Mr Evans,

Online Crime Working Group - 27 November 2014.

Thank you for the opportunity to represent FALCON and the Organised Crime Command at the Online Crime Working Group meeting.

In response to your letter (8 December), I write to provide the Working Group with the key performance indicators for FALCON. I also provide information on the numbers of new and existing police officers who have attended cyber crime training.

Please find two documents attached. In the first, I list the key performance indicators. These may develop and change as FALCON grows. In the second, I outline cyber crime training progress since the inception of FALCON.

Please do not hesitate to contact me should you require any further assistance or information.

Yours Sincerely,

pp. Q Shah (Operational Development, FALCON, SCO7)

Det. Superintendent Jayne Snelgrove.

FALCON

FRAUD AND LINKED CRIME ONLINE

FALCON Key Performance Indicators

What we will measure to ensure we are reaching our goals (Internal use):

- Number of disseminations accepted from Action Fraud
- Number of outcomes in response to Action Fraud referrals (a target of 35% for 14/15 to 50% thereafter - up from 0.45%)
- Value of assets seized/disrupted (£m) as a result of quantifiable interventions against fraudulent activity
- Number (of victims for which) and amount of compensation awarded to victims
- Amount of assets / money obtained through fraud & cyber restrained and prevented from loss
- Number of proactive prevention/enforcement initiatives against business crime
- Number of individuals arrested for fraud & cyber crime offences (a four-fold increase as compared to pre-FALCON)
- Number of individuals charged with fraud & cyber crime offences (a four-fold increase)
- SD rate for fraud & cyber crime (to be best in most similar force grouping. This consists of MPS, West Midlands, Greater Manchester & West Yorkshire).
- Number of active mapped OCGs for fraud & cyber crime (all bands)
- Number of approved disruptions of OCGs (all bands)
- Number of mapped OCG disruptions for fraud & cyber crime where the harm assessment has been reduced.
- Business satisfaction through MOPAC survey

NB: the majority but not all of these will feature in the 14/15 SCO score card. Some data used for these performance measures is sensitive and hence will not routinely be published.

FALCON
FRAUD AND LINKED CRIME ONLINE

FALCON training

1. Mainstream Cyber Crime training.
Prior to FALCON, no staff had received this training.
Currently 59 officers have been trained. A further 72 are due to be trained by the end of the financial year, taking the total to 131.

2. Firebrand / Digital networking and security.
28 officers have been trained thus far. A further 56 are due to be trained by the end of the financial year, taking the total to 84.

3. NCALT cyber crime e-learning programme.
Designed by MPCCU (now FALCON) officers working in conjunction with the College of Policing & NCALT. The first column shows national completions and the second column shows the number of completions in the MPS.
This training is mandatory for all FALCON officers.
FALCON has recently successfully bid for this training to be made mandatory for all MPS staff with public contact and/or investigative duties. As a result, the number of MPS completions is expected to rise significantly before the end of the financial year.

Course Name	Total Completions	MPS completions
Digital Communications, Social Media, Cyber Crime and Policing	**25,888**	**4,742**
Cyber Crime and Digital Policing: Introduction	**36,649**	**3,535**
Cyber Crime and Digital Policing: First Responder	**32,367**	**3,156**
Cyber Crime and Digital Policing: Investigation	**25,267**	**2,473**

4. Other.
By the end of the financial year, a further 24 staff will be trained in mobile phone forensics and 37 in financial investigation (25 FIO, 12 FI).

City of London Police submission to the Online Crime Working Group, March 2015

1. **How do you assess the scale of cyber-enabled acquisitive crime, such as online theft and fraud, that is occurring in London?**

Action Fraud is the UK's national fraud and cyber reporting centre for individual victims and businesses and is designed to receive and assess all reports of fraud and cyber across the UK as one central repository in order to facilitate the development of a better understanding of the national picture of fraud and cyber criminality.

Action Fraud reports are reviewed within the National Fraud Intelligence Bureau (NFIB), hosted by the City of London Police, to make sure fraud and cyber reports reach the right place for enforcement, intelligence or disruption activity. In order to provide a more intelligence led response in developing targeted activity against fraud and cyber crimes, a number of cross sector intelligence streams feed into the NFIB system to add value and enrichen the threat picture to allow a more coordinated response. This allows the NFIB to analyse millions of reports of fraud and cyber collected from the public, small businesses and the public and private sectors, to identify serial offenders, Organised Crime Groups (OCGs) and established and emerging crime types.

On the 1st April 2014, Action Fraud was formally transitioned under ownership of the City of London Police to create a unified fraud and cyber crime reporting centre and intelligence development hub. This new considated service has made a substantial contribution to evidencing the wide harm and complexity of fraud and cyber crime both across London and the wider UK.

This evidence base has informed the Coalition government drive for a stronger focus on fraud and cyber crime, through dedicated capability within the National Crime Agency (The National Cyber Crime Unit and an Economic Crime Command) and also regional capabilities. The approach of these functions is guided by the National Crime Agency mission, following four pillars;

- Pursue those responsible for crime
- Prevent people becoming involved in crime, raising awareness of the corrosive impact, reducing public tolerance
- Protect the public from crime by reducing vulnerabilities
- Prepare the UK for the impact and ensure that the criminal

The delivery of this end to end service by the CoLP has delivered a number of key achievements:

- Development of a comprehensive understanding of the key fraud and cyber threats to establish partnership priorities and design evidence based prevention, disruption and enforcement activities that deliver on public value.

- Provided a single point of contact for all victims of fraud and cyber in the UK, in providing a professional and efficient level of customer service.
- The ability to identify organised criminality operating across sub-sectors and industries to ensure a priorities holistic and coordinated response is provided by law enforcement. The NFIB now disseminated over 6000 crimes a month to UK law enforcement for investigation.
- Establish the intrinsic links between fraud and cyber criminality, identifying cross-cutting enablers for immediate disruption to an estimated prevention of value per annum at over £300 million.
- Identify and map for action, key Organised Crime Groups (OCGs) operating across the fraud and cyber space.
- To understand and respond to real-time threats, to ensure rapid prevention measures are employed to prevent repeat and emerging victimisation
- Increased interoperability and collaboration within and between organisations, both nationally and internationally.
- Optimising the efficient use of available resources and the precision and timeliness of available information for cyber security and business operations.
- Provided a policing model that has shown tangible efficiency savings.

Is there evidence that online theft and fraud are replacing more traditional types of crime such as MOPAC 7 priority crimes?[1]

KEY FINDINGS

The Annual Fraud Indicator (AFI) produced by the National Fraud Authority (NFA) provides one of the most authoritative pieces of research in trying to establish the true scale of fraud, combined from both reported and unreported fraud across sectors. It involved a lot of research and engagement with a number of victim support services, and sub-sector/industry bodies who can report frauf. The most recent and last was produced in June 2013 and provided data for the previous calendar year. It provides an indication of the estimates of the identified cost of fraud and a hidden fraud loss by sector.

Dealing only with loss: the AFI provides a loss to Individuals of £9.1 billion and to the private sector of £5.2 billion (£500m removed as this was marked as Financial and Insurance fraud, covered by CIFAS, FFA (UK) and Insurance Fraud Bureau). The AFI does not deal with number of crimes just projected values of loss.

In relation to what is recorded by Action Fraud and the NFIB, between April 2013 and March 2014, 211,000 crimes with a reported loss of £2.2 billion was documented. 80% (168,800) of these crimes were individuals and 20% (42,200) from business victims, which equates to £1.76 billion individuals and £0.44 billion business assuming that the losses are proportional.

[1] In the Police and Crime Plan 2013-16, the Mayor challenged the Metropolitan Police to reduce seven high-volume, victim-based crimes by 20 per cent. These seven crimes are: burglary, vandalism, theft of and from motor vehicles, violence with injury, robbery and theft from the person.

This leaves a shortfall from the AFI of £7.34bn for individuals and £4.76bn for business. A total of £12.1bn. From the Action Fraud and NFIB figures from the 2013 – 2014 Financial Year this would equate to an additional 703,972 for individuals and 456,527 for business. This provides a projected under reporting of over **1,160,500** crime reports.

Regarding Financial and Insurance Fraud (£500mn, AFI), the CIFAS publication ***Fraudscape*** published in March 2014 deals with volumes of crime and not loss. https://www.cifas.org.uk/employeefraudscape_aprilfourteen CIFAS transfer all of their confirmed fraud to the NFIB and from April 2013 to March 2014, CIFAS reports 233,000 crimes into NFIB (CIFAS data feed is not currently police recorded crime but is recorded as crime under ONS).

The FFA(UK) publication ***Fraud the Facts 2014*** deals with loss and not number of crimes. www.financialfraudaction.org.uk In this publication FFA UK sight a figure of £328.4mn estimated fraud loss within the UK. The data transferred to the NFIB, which was approximately 100,000 crimes between April 2013 and March 2014, does not represent all of this fraud and is only a proportion of this total loss.

KEY FINDINGS

- A high volume of fraud is considered to be unreported.

- NFIB knowledge has highlighted Online Shopping and Auctions and Other Advance Fee Frauds as high volume offences for the individual during 2014. Cheque, Plastic Card and Online Bank Accounts (not psp), Telecom Industry Fraud and Application Fraud are the high volume fraud offences for the private sector.

- Investment fraud and courier fraud are seen as high impact frauds for the individual, often affecting elderly or vulnerable people.

- Mandate fraud and retail fraud are considered to be examples of high impact frauds for the private sector.

- The NFIB has assessed that the key enablers to fraud nationally are the use of identities, social engineering, consumer behaviour and technological / cyber, professional and financial enablers.

- The majority of traditional frauds have been eclipsed by an internet enabled variant and all forms of legitimate internet commerce and retail are subject to fraud. There are few crime categories which do not contain an offence which was cyber enabled.

- Business Process Outsourcing, particularly enabled by VOIP provision, is particularly high in volume of offences and often targets vulnerable members of society. Typically, overseas call centres cold call victims and offer services that they either do not require or that do not then appear in exchange for an advance fee.

- Spoofing is an increasing phenomenon in fraud and occurs where fraudsters use technology to mimic the genuine telephone numbers and email addresses of financial institutions, businesses and government organisations

- The NFIB has largely concentrated on two financial enabler workstreams, money mules and cashless products, and as such observations mainly follow these two areas.

    - The use of money mule networks can be observed across multiple fraud types. The NFIB is working in partnership with FFA UK on a joint money mule strategy which seeks to identify enforcement, disruption and prevention opportunities.

  - The NFIB have been working in partnership with the NCA to assess the exploitation of prepaid cards (PPCs). Although the current PPC intelligence picture is poor there is evidence to suggest that serious and organised criminals are operating on an international level, are utilising PPCs to facilitate and launder the proceeds of crime due to the levels of anonymity afforded by them.

- Identity crime is a key enabler to almost every NFIB coded crime. Fraudsters commit identity crime by stealing the victim's personal information, and then use these details to open bank accounts and obtain credit cards, loans and state benefits. They also order goods in the victim's name, take over the victim's existing accounts, take out mobile phone contracts and obtain genuine documents such as passports and driving licenses in the victim's name.

- Fraudsters work tirelessly to exploit any possible human and systematic characteristics to make some form of financial or personal gain.

- Using common social engineering techniques and basic research, criminals are able to build a relationship with the victim in order to convince them to part with their money.

Advancing technology will continue to enable fraud, and expand the tools available to fraudsters. The increase in the deployment of malware and attributed identity fraud will be facilitated by a continuing lack of knowledge across the general public

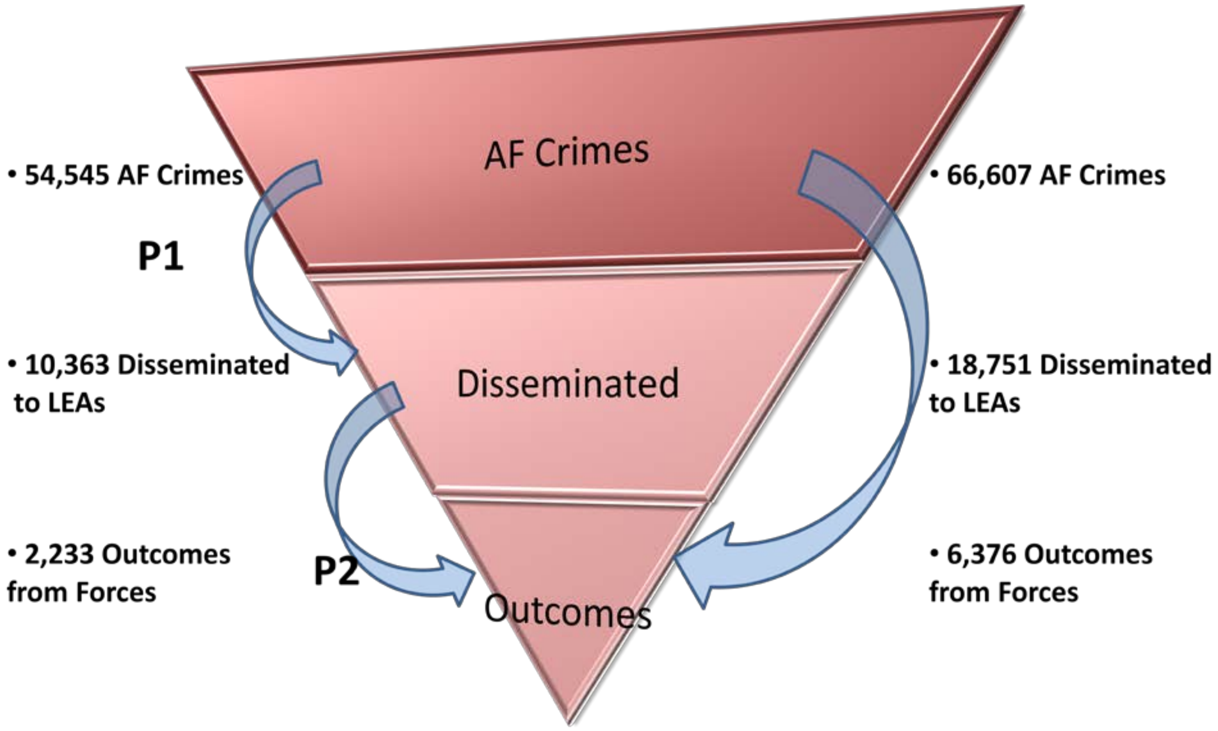
Police recorded crime figures for individual quarters, April 2012 - Mar 2014

England and Wales

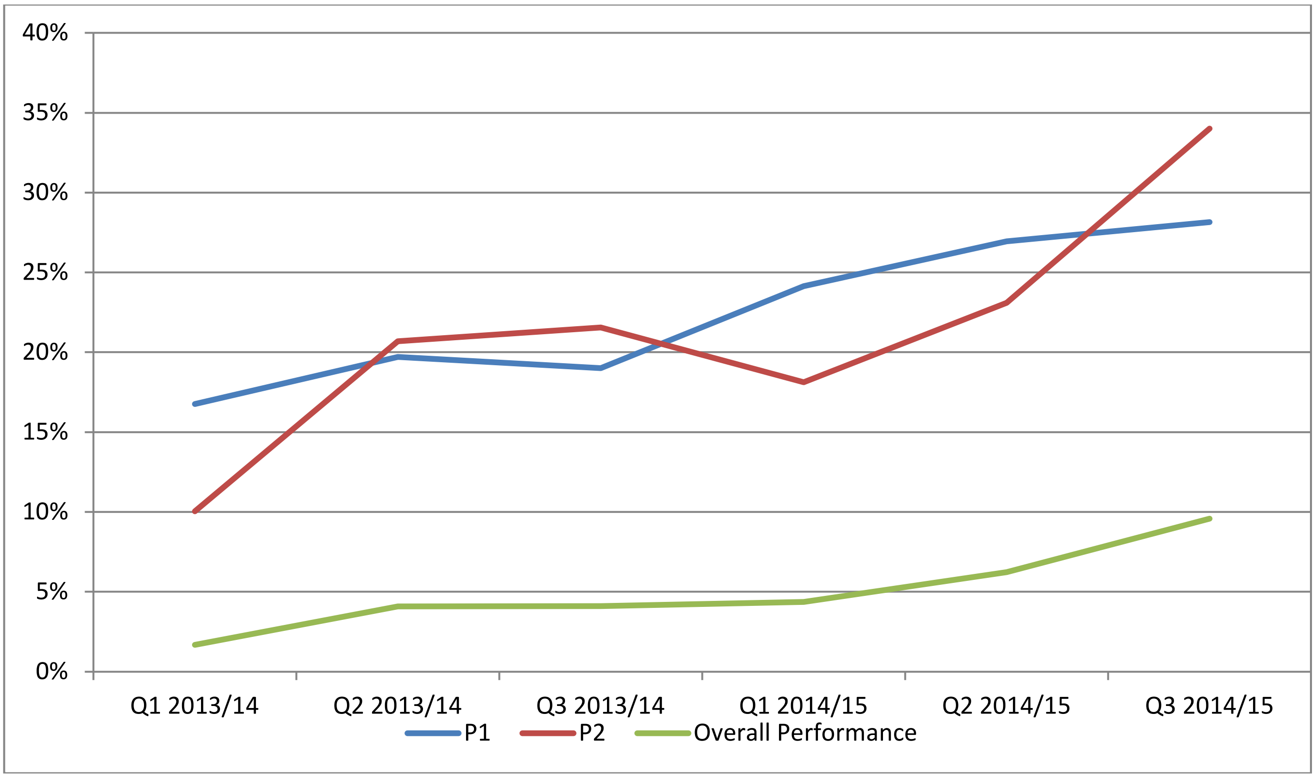
Offence group	2012-13	2013-14	Difference
Violence against the person - with injury	311,945	322,737	103.46%
Robbery offences	65,170	57,814	88.71%
Burglary offences	459,778	443,187	96.39%
Theft of a motor vehicle	79,850	75,308	94.31%
Theft from a vehicle	285,055	276,352	96.95%
Theft from the person	109,807	98,272	89.50%
Criminal damage offences	533,545	505,986	94.83%

2012-13	122,240
2013-14	230,845

3. To what extent are perpetrators getting away with crimes unpunished?


AF Crimes
Disseminated
Outcomes
P1
P2
• 54,545 AF Crimes
• 10,363 Disseminated to LEAs
• 2,233 Outcomes from Forces
• 66,607 AF Crimes
• 18,751 Disseminated to LEAs
• 6,376 Outcomes from Forces

	A	B	C	B/A	C/B	C/A	A/B	B/C	A/C
					Percentages			Ratios	
	Crimes	Disseminations	Outcomes	P1	P2	Overall Performance	P1	P2	Overall Performance
Q1 2013/14	57,736	9,674	971	17%	10%	2%	5.97	9.96	59.46
Q2 2013/14	58,255	11,483	2,375	20%	21%	4%	5.07	4.83	24.53
Q3 2013/14	54,545	10,363	2,233	19%	22%	4%	5.26	4.64	24.43
YTD	**170,536**	**31,520**	**5,579**	**18%**	**18%**	**3%**	5.41	5.65	30.57
Q1 2014/15	59,184	14,283	2,588	24%	18%	4%	4.14	5.52	22.87
Q2 2014/15	61,679	16,626	3,839	27%	23%	6%	3.71	4.33	16.07
Q3 2014/15	66,607	18,751	6,376	28%	34%	10%	3.55	2.94	10.45
YTD	**187,470**	**49,660**	**12,803**	**26%**	**26%**	**7%**	3.78	3.88	14.64



Outside the AFI there are very few statistical or empirical studies that demonstrate the true scale of fraud involving individual victims. Regarding business crime, a number of sub-sectors and industries provide a number of varying projections about what victimization could look like. However, are two key data sets from Home Office Surveys, 2012 and 2013 ***Commercial Victimisation Survey Nature of Crime Against business***. See: https://www.gov.uk/government/publications/crimes-against-business-commercial-victimisation-surveys.

This survey looked at all associated generic frauds (not thefts) that can happen to make businesses victims in 3 types of ways: fraud by employees, which can include fraud by employees who are not based at the sample premises; fraud by others, covering fraud by another known person, for example customers, distributors or suppliers; and fraud by persons unknown, where a fraud has been detected but it is not possible to ascertain who carried it out.

The headline findings report that, a number of businesses across 4 sectors experienced around 644,000 incidents of fraud during the previous 12 months (2013 calendar year), and 10% of all businesses had been a victim of fraud. It was also found that only 10% of crimes were reported to Action Fraud. A quick assessment shows that 10% of these 644,000 incidents is 64,000 and Action Fraud only reported 42,200 crimes. However, a number of these frauds within this 64,000 total would have been recorded by CIFAS and FFA (UK) as these are financial frauds, and are not included in the Action Fraud total.

Fraud by employees was experienced by 2% of business premises across the four sectors covered by the survey. The most commonly reported type was withholding or, “skimming” takings (for example by taking money from customers that was intended for the business). This made up around a third of fraud by employees (34%), with fraudulent accounting (including fiddling expenses, fraudulent claims for work not done or creating fake payroll records) making up a further 30% of fraud by employees. The remaining proportion was made up of a range of less common types of fraud. These included creating non-existent customers or suppliers with the intention of defrauding the business (10% of incidents) and selling goods or services fraudulently (7% of incidents). Other types of fraud (which made up the remaining 19% of incidents) included receiving inferior or no goods and services at all for personal gain and using a business credit card fraudulently (Figure 1.9).

In around three-quarters (73%) of cases disciplinary action was taken against the employee responsible. **Just 7% of respondents whose premises had experienced fraud by employees said that the most recent incident was reported to Action Fraud**, with a further 85% saying that they had not reported the incident to them as they were not aware of Action Fraud. The remaining 9% said that they had not reported the incident to Action Fraud despite being aware of the organisation. However, 37% of victims said that the incident was reported to the police.

Fraud by others. Around a third (33%) of incidents of fraud by others (ie non-employees) were credit, debit or store card fraud (for example paying with stolen, cloned or invalid cards). Cheque fraud (including forged cheques and cheque overpayment fraud) made up 10% of fraud by others and fraudulent payment claims for goods or services that were not delivered (or not delivered as specified) made up 7%. A large proportion (45%) of fraud by others was made up of a variety of less common fraud types.

Incidents of credit, debit or cheque card fraud by others were most frequently conducted over the phone (42% of most recent incidents) or in person (40%). The remainder were conducted over the internet (18% of incidents). Similarly to incidents of fraud by employees, **just 3% of respondents whose premises had been a victim of fraud by others said that the most recent incident was reported to Action Fraud**, with the majority of all victims (91%) saying that they were not aware of Action Fraud and the remaining 6% saying that they had not reported the incident despite being aware of Action Fraud. However, 39% had reported the incident to the police.

Fraud by persons unknown. As shown in the headline findings report, 4% of business premises across the four sectors had experienced fraud by persons unknown in the 12 months prior to the survey. Credit, debit or store card fraud was by far the most common type of fraud by persons unknown, making up half (50%) of this crime type. Ten per cent of incidents involved forged bank notes and 9% were cheque fraud. Other types of fraud by persons unknown (which altogether made up 23% of incidents) included online banking fraud, diverting payments to a fraudulent account or fraudulent payment claims for goods or services that were not delivered (or not delivered as specified). Of incidents of credit, debit or cheque card fraud by persons unknown, 64% were conducted over the phone, 27% over the internet, and just 9% in person.

Similarly to the other fraud types, **just 4% of fraud by persons unknown was reported to Action Fraud**, with 89% of all victims saying that they were not aware of Action Fraud and the remaining 7% saying that they had not reported the incident despite being aware of Action Fraud. Some 37% of incidents of fraud by persons unknown had been reported to the police.

It is impossible to determine if these under reported frauds are included within the projections from the AFI. At the very least, introducing mandatory fraud reporting into Action Fraud would increase the number of crime reports by **1,160,500 per year** at the very least.

There are a large number of both formal and informal studies that depict the true value of fraud across the many sub-sectors and industries that do, or can, report to Action Fraud but these are inconsistent. More work is needed to assess what those values really are, before the initialisation of a project to map service requirements. Additionally, there is a lack of empirical evidence to dictate the true value of fraud against individual citizens, but some information as to the true value of certain fraud types.

C I F A S

Submission to the Online Crime Working Group – 17 October 2014

Introduction

CIFAS shares data with over 300 organisations from both the public and private sectors in order to prevent fraud and financial crime. We have performed this function for over 25 years.

The majority of our partner organisations share confirmed fraud data (to a standard of proof which would support a report to the police) with us on a reciprocal basis. We also ingest data from a range of other sources which support investigations and profiling, including FOG and Amberhill data, law enforcement alerts, and deaths data. CIFAS also holds Home Office immigration data – codified with the commencement of the Immigration Act.

Operating as a not for profit membership association gives CIFAS an important, impartial, position from which to comment: we stand separate to the individual priorities and agendas of individual organisations and stakeholders.

CIFAS also provides information, advice and a service called Protective Registration to members of the public who are at increased risk of falling victim to fraud and also protects the most vulnerable in society from predatory criminals by leveraging its data for the common good.

On what scale are cyber-enabled acquisitive crimes occurring in London?

Cyber-enabled acquisitive crimes are occurring on a large scale in London. CIFAS' figures reflect only the confirmed frauds which are reported to us, and not those for which such a standard is not met.

Appendix A shows the level of confirmed frauds as seen by CIFAS during 2013/14 in the metropolitan policing area. This shows the type of fraud, the product on which it was attempted, the vehicle through which the fraud took place, and also the number of known victims of fraud.

Despite each of these confirmed frauds being to the level of proof of a crime according to the Home Office counting rules, these figures are not yet included in the Official Crime Survey. This has several knock-on effects which we have detailed below.

How concerned are Londoners about the threat that they face?

CIFAS is of the view that this is impossible to gauge. An unvirtuous circle exists where a lack of awareness fuels a lack of action.

The allocation of police resources will be ultimately set and influenced by both political and public opinion. Without a full picture of the true level of crime in London therefore, the allocation of resource will never meet the reality on the ground.

Similarly, as the levels of confirmed fraud reported to CIFAS (and other bodies) are not included in official statistics the public do not have the full picture of the threat that they face.

An example of this would be through crime maps. While popular with the public and a clear indicator of the level of certain types of criminality in a local area, they do not include fraud data. If crime maps did include show incidences of confirmed fraud, a very different picture would emerge which would, at the very least, serve to alert the public to the threat.

It is fair to say that the public are shielded to a degree from the threat and consequences of financial crime – the costs of fraud are often absorbed by banks and insurers, resulting in higher charges and premiums for all. There is a strong argument that raising awareness of the threat would have not just preventative benefits, but also economic ones.

It is important to give full consideration to how victims of identity crime have changed in recent years. Historically, the traditional target for an identity fraudster was considered to be the obviously affluent, professional male, who would be targeted numerous times by a fraudster across a range of products and services, until their creditworthiness was exhausted. Now, not only are more people targeted than ever before, but the value of the frauds has decreased: meaning a shift from low volume, high value to high volume, lower value frauds has taken place.

During the last decade, particular preventative advice was targeted at people in order to get them to shred all paperwork (thus preventing fraudsters from stealing data) and also specifically at those living in multiple access properties (e.g. those in blocks of flats, students, young professionals etc) as they were deemed to be 'more vulnerable'. CIFAS has challenged what is considered by 'more vulnerable' in two reports, co-authored with Experian[1] and Ordnance Survey[2] to demonstrate that some long held assumptions are not supported by analysis of the data recorded on CIFAS databases.

In short, it is becoming easier to commit fraud and a majority of this criminality now takes place online.

Is there evidence that cyber-enabled acquisitive crimes are replacing more traditional types of crime, such as MOPAC 7 priority crimes?

It would certainly appear that cases of fraud, and especially ID fraud continue to rise while the media reports that 'crime' more generally is falling.

The Committee will be aware of recent media coverage given to falling crime rates over recent years being at odds with rising fraud numbers, and the debates regarding whether all statistics have been collated. For example, *The Times* reported critically recently regarding the private sector not reporting all incidences of financial crime[3]. While organisations should be encouraged to be transparent and report to the police all incidents of fraud, this will only happen when organisations are confident that law enforcement will act on the information it gathers and provides.

It is worth noticing that CIFAS figures alone show an increase from 214,342 frauds identified in 2008 to the region of 250,000 frauds per year in both 2011 and 2012. These, of course, are those frauds that satisfy a legal standard of proof to identify that a criminal fraud act has taken place and should be contrasted against the media reporting that levels of crime continue to fall.

As with any other acquisitive crime, it has to be remembered that there is far more that is unseen as it is not counted or contributed to systems such as CIFAS'.

To what extent are perpetrators getting away with crimes unpunished?

Industry bodies, such as CIFAS, work to disrupt and make hostile the environment for fraudsters and financial criminals. The scale of the issue, and relative ease of committing such a crime, means that law enforcement are not resourced proportionately to investigate and punish such criminality.

The vast majority of fraudsters currently escape unpunished because police must prioritise scarce resources on targeting fraudsters causing the most financial harm to individuals, and on chasing criminals who stand the best chance of being identified and located.

In around two thirds of all frauds reported to NFIB, an organisation is the financial victim, however resources are almost exclusively allocated to reviewing the large and growing number of Action Fraud reports from individual financial victims of fraud. By consequence, although around 81,000 reports of financial fraud against public and private sector organisations were reported to NFIB via CIFAS as occurring within the Greater London area in 2013, NFIB were only able to disseminate 589 of these reports to the Metropolitan Police for investigation, across 112 separate investigations. Of those 112, only 10 investigations resulted in arrests and/or convictions of one or more fraudsters. A further 38 investigations were undertaken but did not result in an arrest or conviction, and 46 investigations were deemed not proportionate for investigation at all, given priorities and available resources at the time.

In addition, more than half of the fraud offences against organisations reported to NFIB via CIFAS in 2013, involved a form of 'identity crime' whereby individuals or companies were impersonated by fraudsters who knew sufficient information about their targets to either apply for new products and facilities in their name, or to hijack their existing facilities. In the vast majority of cases, the true identity of the offender is not known and therefore police have to decide whether or not to undertake lengthy investigations to try and identify and locate where a fraudster is based. Often, even the most able and determined police officer may not be able to achieve this.

[1] **Fraudscape 2014**, Chapter 5. March 2014. Available at:
https://www.cifas.org.uk/secure/contentPORT/uploads/documents/CIFAS%20Reports/External-CIFAS-Fraudscape-2014-online.pdf

[2] **Identity Crime: On Your Doorstep**. October 2013. Available at:
https://www.CIFAS.org.uk/secure/contentPORT/uploads/documents/External-IDcrime_onyourdoorstep_CIFAS_OS.pdf

[3] Met chief acknowledges scale of online fraud, The Times, 28 August 2014:
http://www.thetimes.co.uk/tto/news/uk/crime/article4189257.ece

Is the Met prioritising its resources appropriately to deal with the threat of cyber-enabled acquisitive crimes and how does it need to adapt to this new threat?

CIFAS supports the Met's prioritisation of resources to deal with the threat of cyber-enabled acquisitive crimes. In CIFAS' view, however, political leaders must take a view on the likely future increase in cyber criminality and direct policing resource accordingly.

Realistically, the Met is only able to do what they are given to do (please refer to the previous answer). The rollout of cases from the NFIB to the Met, therefore, will largely determine what actions will be taken, by whom and the resources that are available to support such actions.

CIFAS very much welcomes the launch of FALCON, the mission of which is to reduce the harm caused by fraud and cyber criminals in London. CIFAS is keen to assist and support the work undertaken by FALCON in any way that it can and strongly urges the Met to make use of the specialisms and expertise that already exists within the fraud prevention community spread across private, public and third sectors. Similarly, the Met's work with Operation Sterling (which examines the enablers in an attempt to try and do something about the crime) is to be applauded and can be enhanced by making use of the vast expertise that exists outside of the police force.

The publication of the government's Serious Organised Crime Strategy in October 2013 outlined a strategy defined by the "4 Ps: Pursue (prosecuting and disrupting serious and organised crime), Prevent (preventing people from engaging in serious and organised crime), Protect (increasing protection against serious and organised crime), and Prepare (reducing the impact of serious and organised crime). It is important to bear in mind that a similar approach has been used by the Met, so in terms of how the Met prioritises its resources, CIFAS is of the opinion that the Met police have taken positive steps to tackle such crime.

Ensuring that the Met has the right people, with the right skills, who are given the right technical resources in support will be the main priority, and CIFAS repeats its belief that the expertise (not just the data) available from private and public sector organisations could help to strengthen the Met's response. The question of training and awareness within the police force will also be of paramount importance, as the pace of technological development drives the evolution of cyber-enabled crimes it is important that those fighting the crimes are equally fast in developing counter fraud techniques.

CIFAS would submit that the Committee should consider whether everything being done, within the law and through the law, to counter cyber criminals and fraudsters? The non prosecution of identity fraudsters, and the fact that individual victims of identity fraud or theft are not seen as 'victims' is a message that will seriously undermine any strategy, no matter how effective.

How can we improve how cyber-enabled crimes are measured and reported?

Clear definitions are required to properly measure the scale of the cyber crime threat.

CIFAS is of the view that a clearer definition of what is deemed "cyber enabled crimes" is fundamental before any potential improvements are made to how such crimes are measured and reported. Is a cyber enabled crime - for example - a spam email? A listing for a counterfeit good on an auction site? Or is it the use of a computer/device/internet/hacking/network intrusion/malware etc in order specifically to commit criminal activity such as fraud against an organisation or group of individuals?

Currently, without a clearly set out definition of what is to be counted and what is not, measurement and reporting of cyber-enabled crimes will be impeded. Upon the adoption of a clear set of definitions, CIFAS considers it vitally important for all organisations and bodies (financial services, small and medium enterprises, public sector and third sector) to be encouraged or even compelled to share fraud data and contribute. Equally, law enforcement should undertake to provide clear feedback and pursuit of identified cyber criminals in order to guarantee the continued contribution of such data.

Fraud must not become a competitive issue - as no advantage is to be gained by not working together - but bringing data and measurements together will require, also, agreement on a shared set of expectations and commitment to fulfilling such expectations.

Are there examples of best practice both nationally and internationally of dealing with the cyber threat?

Criminals work better together than industry, government or law enforcement. To tackle this issue, a truly cross-sector approach needs be taken, removing any competitive element from fraud prevention.

Law enforcement offerings such as the Business Crime Resilience Centre and the Security and Prevention Advice services offered to businesses and the public are excellent examples of how educative and informative messages can be rolled out to engage the wider public community in preventative measures. Equally, organisations like CIFAS have brought together over 300 organisations to share fraud data for the specific purpose of preventing further fraud. The existing strategies and the dedication to the 4 Ps, therefore, are to be applauded as the strategy is focused upon dealing with the cyber threat.

Appendix A - **level of confirmed frauds as seen by CIFAS during 2013/14 in the metropolitan policing area**

Type of fraud	2013	Proportion	2014 (to Sep end)	Proportion
Asset Conversion	55	0.1%	48	0.1%
Application Fraud	10,159	12.6%	7,073	10.8%
False Insurance Claim	99	0.1%	83	0.1%
Facility Takeover Fraud	11,670	14.4%	5,565	8.5%
Identity Fraud	37,963	47.0%	27,077	41.2%
Misuse of Facility	20,874	25.8%	25,853	39.4%
Total	80,820	100.0%	65,699	100.0%

Product	2013	Proportion	2014 (to Sep end)	Proportion
All-in-One	103	0.1%	62	0.1%
Asset Finance	1,408	1.7%	1,153	1.8%
Bank Accounts	24,046	29.8%	21,872	33.3%
Communications	10,343	12.8%	13,628	20.7%
Insurance	3,225	4.0%	1,722	2.6%
Online Retail	11,037	13.7%	3,967	6.0%
Plastic Cards	24,185	29.9%	16,082	24.5%
Mortgage	1,414	1.7%	1,166	1.8%
Loans	3,819	4.7%	4,057	6.2%
Other	1,240	1.5%	1,990	3.0%
Total	80,820	100.0%	65,699	100.0%

Delivery	2013	Proportion	2014 (to Sep end)	Proportion
Broker	1,547	1.9%	1,250	1.9%
Combination	3,975	4.9%	2,404	3.7%
Dealer	2,592	3.2%	1,751	2.7%
Face to Face	10,826	13.4%	14,017	21.3%
Mail	2,600	3.2%	2,161	3.3%
Internet	43,211	53.5%	31,708	48.3%
Other	4,593	5.7%	2,187	3.3%
Retailer	1,890	2.3%	1,344	2.0%
Telephone	9,586	11.9%	8,877	13.5%
Total	80,820	100.0%	65,699	100.0%

Victims	2013	Proportion	2014 (to Sep end)	Proportion
Victims of Impersonation	29,591	84.4%	22,336	88.6%
Victims of Takeover	5,461	15.6%	2,863	11.4%
Total	35,052	100.0%	25,199	100.0%

LONDONASSEMBLY
Chairman of the Online Crime Working Group

City Hall
The Queen's Walk
London SE1 2AA
Switchboard: 020 7983 4000
Minicom: 020 7983 4458
Web: www.london.gov.uk

Our ref : 2014-15/33
Your ref :
Date: 24 October 2014

The Rt Hon Norman Baker MP
Minister of State for Crime Prevention

(Sent by email)

Dear Norman,

Members of the London Assembly's Police and Crime Committee have established a Working Group to investigate how online theft and fraud is tackled in the capital. As part of our investigation, we are collecting what available data there is on victims of these crimes.

At the Working Group's first meeting on 21st October 2014, we were told that in recent years, the Crime Survey for England and Wales has asked respondents about their experiences of online crime.[1] In particular, the 2011-12, 2012-13 and 2013-14 questionnaires all asked respondents whether they had, in the previous 12 months, personally experienced a range of potentially criminal activities while online (please see the appendix for more detail).

Fraud and cyber-crime – including some of the other examples given in the question – are not currently included in the survey's main estimates of crime. The Office for National Statistics (ONS) says that it has "not been possible to incorporate these [crime types] into the headline figures due to different data collection approaches and challenges around measuring fraud and cyber-crime".[2] However, the ONS has not yet published the results for the above question separately from the main survey in any of the past three years. As this data has been collected we would like these results to assist us with our investigation.

I set out our detailed requests in the appendix to this letter; I would be grateful if you would pass on these requests to your officials to action.

We would be grateful if this information could be provided by **Friday 21st November 2014**, copying in Dan Maton, Budget & Performance Adviser at the London Assembly, to your response (dan.maton@london.gov.uk; 020 7983 4681).

[1] Meeting of the London Assembly's Online Crime Working Group, 21st October 2014.
[2] Office for National Statistics, Methodological note: Work to extend the Crime Survey for England and Wales to include fraud and cyber-crime, 16 October 2014.

Yours sincerely

Roger Evans AM
Chairman of the Online Crime Working Group

Appendix – Detailed request for data

The London Assembly's Online Crime Working Group is making two requests for data collected in the Crime Survey for England and Wales. These are set out below.

The following question was included in the 2011-12, 2012-13 and 2013-14 adult questionnaires:

Extract from the Crime Survey for England and Wales adult questionnaire, follow-up module D (2011-12, 2012-13 and 2013-14):[3]

Question name: EEXPINTA – EEXPINTH

LIGHT BLUE SHOWCARD D3
In the last 12 months, have you personally experienced any of the things mentioned on this card while using the Internet?
1. A computer virus
2. Loss of money
3. Unauthorised access to/use of personal data (e.g. e-mail account/bank account)
4. Upsetting images/illegal images
5. Abusive/threatening behaviour
6. None of these

REQUEST 1: Please provide the results to the above question for 2011-12, 2012-13 and 2013-14 in Excel format. If possible, please break down the data for each year by region – in particular, we would like to know the prevalence of these crimes in London compared to the rest of England and Wales.

The 2013-14 adult questionnaire included a series of follow-up questions in addition to the above. These questions are set out below:

Extracts from the Crime Survey for England and Wales adult questionnaire, follow-up module D (2013-14 only):

Question name: EEXPLOSS
You said that you personally experienced loss of money in the last 12 months as a result of using the internet. How much money did you lose?
Please DON'T include any money that was subsequently refunded by your bank, building society or credit card company but DO include any additional charges or costs that you incurred as a result of the incident
IF NEEDED: PLEASE THINK ABOUT ALL THE WAYS IN WHICH YOU LOST MONEY AS A RESULT OF USING THE INTERNET IN THE LAST 12 MONTHS AND PROVIDE A TOTAL AMOUNT
1. None (i.e. all money was refunded)
2. Less than £50
3. £50 - £99
4. £100 - £249
5. £250 - £499
6. £500 - £999

[3] The 2011-12, 2012-13 and 2013-14 Crime Survey for England and Wales adult questionnaires are available on the ONS website: http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/questionnaires/index.html

7. £1,000 - £2,499
8. £2,500 - £4,999
9. £5,000 or more
10. Not yet resolved

Question name: ELOSREPA – ELOSREPK
LIGHT BLUE SHOW CARD D5
Did you report this loss of money to anyone? CODE ALL THAT APPLY
INTERVIEWER NOTE: IF EXPERIENCED MORE THAN ONE LOSS, THINK ABOUT THE LAST OCCASION
1. The police
2. Anti-virus software company
3. Internet service provider
4. Your bank, building society, or credit card company
5. Action Fraud
6. Other government agency
7. Website administrator (e.g. Facebook, eBay)
8. Someone else
9. No-one

Question name: ELOS2REP
LIGHT BLUE SHOW CARD D5
Who did you FIRST report the loss of money to?
CODE ONE ONLY
1. The police
2. Anti-virus software company
3. Internet service provider
4. Your bank, building society, or credit card company
5. Action Fraud
6. Other government agency
7. Website administrator (e.g. Facebook, eBay)
8. Someone else

Question name: ELOSSAT
Overall, were you satisfied or dissatisfied with the way [TEXTFILL: Answer from ELOSREP2, or ELOSREP if only one selected] handled this matter?
INTERVIEWER: IF SATISFIED ASK: Very satisfied or just fairly satisfied?
IF DISSATISFIED ASK: A bit dissatisfied or very dissatisfied?
1. Very satisfied
2. Fairly satisfied
3. A bit dissatisfied
4. Very dissatisfied
5. SPONTANEOUS ONLY: Too early to say

REQUEST 2: Please provide the results to the follow-up questions set out above from the 2013-14 adult questionnaire in Excel format. If possible, please break down the data for each year by region – in particular, we would like to know the prevalence of these crimes in London compared to the rest of England and Wales.

Appendix 1

Home Office

Rt Hon Lynne Featherstone MP
Minister for Crime Prevention

2 Marsham Street,
London SW1P 4DF
www.gov.uk/home-office

Roger Evans AM
City Hall
The Queen's Walk
London SE1 2AA

Your ref: 2014-15/33
CTS ref:

18 November 2014

Dear Mr Evans,

Thank you for your letter of 24 October to my predecessor, Rt Hon Norman Baker MP, about data from the Crime Survey for England and Wales (CSEW) relating to online crime and fraud.

Responsibility for the Crime Survey passed from the Home Office to the Office for National Statistics (ONS) in 2012, following the National Statistician's independent review of crime statistics. My officials have spoken to their ONS counterparts, and I understand that the ONS has now published the figures you request on its website (at http://www.ons.gov.uk/ons/about-ons/business-transparency/freedom-of-information/what-can-i-request/published-ad-hoc-data/crime/november-2014/index.html).

The Crime Survey questions you referred to capture information on users' 'negative online experiences'. Whilst the resulting data provides a useful indicator, the data is not included in the headline crime count of the survey, as it does not directly measure criminal activity or police recorded crime (i.e. some 'negative online experiences' will be unpleasant but not criminal).

The Home Office takes cyber crime and fraud very seriously, and we are working closely with the ONS to improve the measurement of both in the Crime Survey. In the meantime, we use a range of published data to build up our picture of the issues.

Yours sincerely

Kind Regards

Rt Hon Lynne Featherstone
Minister of State