LONDONASSEMBLY

Online Crime Working Group – Summary of site visit to City of London Police on 26 November 2014

Attendees

Assembly Members	Roger Evans AM (Chairman) Joanne McCartney AM Caroline Pidgeon MBE AM Jennette Arnold OBE AM Tony Arbour AM
London Assembly staff	Dan Maton, Rachel Roscow, Mary-Clare Walsh, Daniel Woolf
Visiting	Commander Steve Head, National Police Coordinator for Economic Crime, City of London Police Detective Superintendent Peter O'Doherty, Director of National Fraud Intelligence Bureau, City of London Police

Overview of visit

The Online Crime Working Group visited the City of London Police's (CoLP) Economic Crime Division on 26 November 2014. It received a briefing from Commander Steve Head about the work that the City of London Police do to tackle online crime. The Working Group also received a briefing from Detective Superintendent Peter O'Doherty about the work of the National Fraud Intelligence Bureau (NFIB), which is run by the City of London Police. Finally, the Working Group was shown examples of how NFIB disrupts websites, for example those that are seeking to defraud victims, and how it puts together "packages", which are sent to police forces for further investigation.

Key findings

The main purpose of the site visit was to inform the Working Group about the role of the City of London Police – and in particular Action Fraud and NFIB – ahead of its meeting on 27 November 2014. Command Head from the City of London Police attended this meeting as well as representatives from the Metropolitan Police Service and the Mayor's Office for Policing and Crime.

During the visit, the Working Group noted the following points which are relevant to its online crime investigation:

Briefing with Commander Steve Head

- CIFAS – the UK's fraud prevention service – previously told the Working Group that it reported 81,000 financial frauds against organisations in London to National Fraud Intelligence Bureau in 2013. But of these only 589 of these reports were passed to the Met across 112 investigations; and of those 112, only 10 investigations resulted in an arrest or conviction of one or more fraudsters.[1] CoLP said that this information is used to enhance the packages that NFIB send out to police forces to investigate and make them more viable. It also said that NFIB's disruption teams use the CIFAS data – which can include perpetrators' banking details and phone numbers. CoLP said that, intuitively, it thinks many of the 81,000 reports are crimes.

[1] CIFAS submission to the Online Crime Working Group, 17 October 2014.

- "Bulk reporting" will be introduced to encourage businesses that have a high volume of transactions to report fraud. Currently, some large businesses make a commercial decision not to report fraud. The new system – planned to go live in December 2014 – should allow these organisations to report up to 250 incidents at once. This will help the police to identify patterns and networks of criminals.
- CoLP said there is an issue about the capability of police forces in responding to fraud and online crime. They need to think about prevention and disruption too.
- Businesses also need to think about how they might need to change their working practices to deter fraudsters (e.g. websites that sell tickets). Individuals need to protect themselves online as well – people lock their front doors, they need to apply the same principles online.
- In the past, police forces investigated each reported fraud in isolation (or not at all). Five years ago, forces viewed fraud as a low priority, but it is increasingly seen as a problem. CoLP is seeing a "huge rise in reporting", but it is still important to raise awareness about Action Fraud – the central reporting service for fraud and online crime – as many people do not know what it is or what it does.

Briefing with Detective Superintendent Peter O'Doherty

- In 2005, the quality of fraud investigation by the police service was very low and there was little or no training for police officers on how to investigate fraud.
- Action Fraud was established predominantly for individuals and small and medium enterprises (SMEs) to report fraud and online crime.
- NFIB takes reports from Action Fraud and uses an algorithm to score crime reports. This is based on four key questions:
    - Can police forces investigate the crime?
    - Can they solve it?
    - What level of harm has been done?
    - Are there repeat and/or vulnerable victims?
- Action Fraud receives around 21,000 reports every four weeks across 55 categories of fraud (six are cyber-dependent fraud). Around 70 per cent of frauds are now cyber-enabled, up from 40 per cent in recent years.
- NFIB uses disruption techniques – it can shut down a website within 48 hours. If crime reports are not used for disruption or enforcement, NFIB use them as intelligence to inform prevention work.
- In addition to "bulk reporting", another new system which is being launched is a multi-session reporting system so individuals can report online crimes and track what is happening with their report in the system.
- The police service in England and Wales still has limited capability to police fraud and online crime. Police forces need to gain new skills – officers need to be comfortable investigating crimes on the internet. CoLP now produces "fraud profiles" every quarter for each police force in England and Wales.
- The Met's response to tackling fraud has been low compared to other, but CoLP is encouraged by the Met's new Fraud and Linked Crime Online (FALCON) command.
- Specials have been useful at providing police forces with their expertise (particularly those with backgrounds in finance and/or ICT).
- Previously, victims of fraud did not always receive a response from the police. Now, CoLP sends a letter to all victims that report to Action Fraud.
- CoLP now sends cases to police forces that could total £10 million, rather than individual crimes that might only be for a few thousand pounds.

- Intelligence led policing is needed. Traditional enforcement alone will not work because suspects are often unreachable (if they are based in Russia for example).
- CoLP values the cost to the police of disruption tactics at £11.1 million, but the value of this work saves around £300 million.
- Action Fraud is increasingly becoming more recognised, last year the Action Fraud website had over 3 million visitors, the team received 1.8 million calls and they currently have around 14,000 Twitter followers. But, given the scale of the threat, fraud and online crime might need to become a tier one threat, with campaigns on a par with those for drunk driving to raise awareness further. CoLP plans to launch targeted campaigns – one recent example is its "12 frauds of Christmas" campaign.