Subject: Online Crime

Report to: Online Crime Working Group	
Report of: Executive Director of Secretariat	**Date: 27 November 2014**
This report will be considered in public	

1. Summary

1.1 This report provides background information to the second meeting of the Online Crime Working Group. This Working Group will gather evidence on behalf of the London Assembly's Police and Crime Committee for use in its investigation into online crime in London.

2. Recommendation

2.1 **That the Working Group notes this report as background to putting questions to invited guests on online crime in London and notes the discussion.**

3. Background

3.1 At its meeting on 9 October 2014, the London Assembly's Police and Crime Committee agreed to establish an Online Crime Working Group to gather evidence on its behalf. The size, membership and chairing arrangements of the Working Group, as agreed by the Committee on 9 October 2014, are as follows:

- Roger Evans AM (Chairman);
- Jennette Arnold OBE AM;
- Tony Arbour AM;
- Joanne McCartney AM; and
- Caroline Pidgeon MBE AM.

3.2 The Police and Crime Committee agreed the following term of reference for the Working Group:

To gather evidence on behalf of the Police and Crime Committee on the Mayor's Office for Policing and Crime (MOPAC) and the Metropolitan Police Service (MPS) response to the new threat that cyber-enabled crimes present and report back to the Committee, which may then make recommendations on this issue.

3.3 The Police and Crime Committee agreed the following terms of reference for the investigation on 9 October 2014:

- To examine MOPAC and the MPS's localised response to tackling cyber-enabled acquisitive crimes against individuals through the MPS new Fraud and Linked Crime Online (FALCON) command;
- To review these approaches against any established best practice for policing cyber-enabled acquisitive crimes – including prevention, response and justice for victims – and assess whether they are adequate; and
- To assess levels of reporting and public awareness about cyber –enabled acquisitive crimes in London.

3.4 The scoping paper that the Police and Crime Committee agreed at its meeting on 9 October 2014 for this investigation is available here.[1]

3.5 The Online Crime Working Group will report its findings back to the Police and Crime Committee.

3.6 Crimes committed using the internet, often referred to as 'cyber-crimes', are a new and pressing threat. Many crimes, both old and new, can now be committed using the internet and are therefore considered a 'cyber-crime'.

3.7 Broadly, there are two categories of cyber-crime:

- **Cyber-dependent crimes** are offences carried out using new technologies in violation of the Computer Misuse Act 1990, such as hacking email accounts and denial of service attacks.[2] The police response for tackling cyber-dependent crimes is led predominantly at a national level, through the National Crime Agency.
- **Cyber-enabled crimes** are traditional crimes which can be increased in their scale or reach through the use of computers, computer networks or other ICT, including mobile phones (examples include online fraud and identity theft).[3]

3.8 Since the police response for tackling cyber-dependent crimes is led predominantly at a national level, through the National Crime Agency, the Working Group's investigation will focus on **cyber-enabled crimes** against individuals that are policed at the force level. And since most crimes can have a 'cyber-enabled' element, the Police and Crime Committee agreed that the Working Group will focus on crimes with an economic or financial incentive (known as acquisitive crimes).

3.9 Some examples of cyber-enabled acquisitive crime are:

- Electronic financial frauds, most notably online banking frauds and internet enabled card-not-present (CNP) fraud.
- Fraudulent sales through online auction or retail sites or through bogus websites, which may offer goods or services that are not provided or are counterfeit/misrepresented.

---

[1] Weblink to the scoping paper: http://www.london.gov.uk/moderngov/documents/s39733/Appendix%201-Online%20crime%20scoping%20paper__FINAL.pdf

[2] A denial of service (DoS) attack is a malicious attempt to make a server or a network resource unavailable to users, usually by temporarily interrupting or suspending the services of a host connected to the Internet.

[3] Cyber-crime: A review of the evidence, Home Office, October 201, weblink: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

- Mass-marketing frauds and consumer scams, where, for example, individuals are persuaded to part with money upfront to help someone or to invest in a business, on the promise that a larger sum of money will be returned to them at a later date.
- 'Online romance' (or social networking/dating website) frauds, where individuals may be contacted via social networking or dating sites and persuaded to part with personal information or money following a lengthy online 'relationship'.[4]

3.10 The number of cyber-enabled crimes is increasing. In England and Wales, 230,000 frauds – many in London – were reported to Action Fraud in 2013/14, almost twice as many as in the previous year.[5] Of these, 70 per cent had a cyber-element, compared to 40 per cent five years ago. But despite the recent increase in reported frauds, the true picture of online crime is unclear. Many of these crimes are still significantly underreported to the police by victims.

3.11 The Metropolitan Police Service (MPS) intends to launch a FALCON command in October 2014. FALCON's remit will include acquisitive crimes. One of its services will be a centralised capability that the MPS hopes will remove the onus of investigation of fraud and cyber-enabled crimes from local policing boroughs and provide a consistent approach to investigations.[6]

3.12 The Online Crime Working Group held the first meeting of its investigation on 21 October 2014. It collected evidence from invited guests about perpetrators of online crime, the scale of the problem in London and the police response to the threat. The Working Group also identified who is most at risk of becoming a victim of online crime and examined issues of why reporting of online crime might be lower than for other crimes.

4. Issues for Consideration

4.1 The following guests have been invited to discuss online crime in London:

- **Alex Marshall QPM**, Chief Executive Officer, College of Policing;
- **Matthew Allen**, Director Financial Crime, British Bankers' Association;
- **Commander Neil Basu**, Metropolitan Police Service;
- **Detective Superintendent Jayne Snelgrove**, Metropolitan Police Service;
- **Detective Superintendent Peter O'Doherty**, Director of National Fraud Intelligence Bureau, City of London Police; and
- **Rebecca Lawrence**, Director of Strategy, Mayor's Office for Policing and Crime.

4.2 This is the final scheduled meeting of the Online Crime Working Group.

---

[4] Cyber-crime: A review of the evidence, Home Office, October 2013, Chapter 2, page 4.
[5] Action Fraud is run by the City of London Police, the national policing lead for economic crime
[6] MPS Briefing Note: Cyber Crime, 2014, weblink: http://www.met.police.uk/docs/cyber-crime.pdf

5. Legal Implications

5.1 The Online Crime Working Group has the power to do what is recommended in this report.

5.2 The Working Group cannot make decisions.

6. Financial Implications

6.1 There are no financial implications to the GLA arising from this report.

List of appendices to this report:
None.

Local Government (Access to Information) Act 1985 List of Background Papers: There are none.	
Contact Officer:	Dan Maton, Budget and Performance Adviser
Telephone:	020 7983 4681
E-mail:	dan.maton@london.gov.uk