LONDONASSEMBLY

The Committee carried out a review of the Met's approach to tackling online theft and fraud in 2014. A working group, chaired by Roger Evans AM, carried out the investigation on the Committee's behalf and the Committee published its report in March 2015.

The table below provides a summary of the impact of each of the recommendations and the extent to which they have been accepted by MOPAC and the Met using RAG (red, amber or green) status. RAG status provides a performance judgment: in this instance, red means the recommendation has not been accepted; amber means there has been some progress against the recommendation; and green means the recommendation has been implemented or substantively accepted.

Committee's recommendation	Response	Progress
Recommendation 1: In the next year, MOPAC should commission criminologists and/or other academics to work with the Met to develop profiles of the different types of perpetrators of online crime that are based in London, in order to help the Met to tailor its response. The research should focus on low-level, high-volume online crimes; it should also pay particular attention to the extent to which perpetrators are currently involved in other forms of offending, or have been in the past.	MOPAC says it is working with Operation Falcon from a crime prevention and target hardening viewpoint. MOPAC will work with the Operation Falcon team seconded to the London Digital Security Centre (LDSC) to assess whether there are particular archetypes of online offenders as seen through those prosecuted. There are currently eight Met Cyber Protect officers seconded into the LDSC team. The LDSC will work with MOPAC's Evidence and Insight team of social researchers to assess whether there are any trends in offending patterns, for example using Police national computer data.	This recommendation has been substantially accepted: MOPAC will take steps to get a better understanding of the profiles of offenders based in London.
Recommendation 2: The Office for National Statistics should introduce specific questions into the Crime Survey for England and Wales to measure online victimisation.	The Minister for Crime Prevention, in her response to the Committee's report, stated that she agreed there is more to do to ensure that crime statistics properly capture online crime. John Flatley, Head of Crime Statistics and Analysis at the	There is some progress against this recommendation: both the Minister and the ONS accepted that we to ensure online crimes are capture in the statistics. It is yet to be seen, however, whether the

Committee's recommendation	Response	Progress
It should include these offences in the Crime Survey's headline results from 2016-17 onwards.	Office for National Statistics, also responded to the Committee's report. He said that the ONS has established a project to explore the feasibility of covering fraud and cyber-crime in the main Crime Survey in the future.	Crime Survey's headline results will include online crimes such as cyber-fraud in the future.
Recommendation 3: The Mayor's Office for Policing and Crime should develop specific questions to capture individuals' online victimisation in London, with a view to introducing them into its quarterly Public Attitudes Surveys from 2016-17 onwards. In addition, MOPAC should extend its Business Attitudes Survey to measure online victimisation among London's businesses. It should publish the headline results from each survey on the London Datastore.	MOPAC says its analysts are assessing whether the new MyVoice survey of victims can include members of the public, and not just businesses. The Business Attitude Survey (BAS) asks businesses about online victimisation. It is in its second wave of interviews. MOPAC will publish its BAS results on the Business crime page of the MOPAC website. The PAS now includes questions about online crime/victimisation.	This recommendation has been accepted.
Recommendation 4: The Mayor, in partnership with the City of London Police and other key stakeholders, should lead a London-wide campaign during 2015-16 to draw attention to the threat of online crime and raise awareness of Action Fraud to improve reporting of crime by	MOPAC says it is working through the LDSC with a number of partners on a series of masterclass briefings for businesses on cyber-crime and fraud. The first was held on 26 May in City Hall, opened by the Deputy Mayor for Policing and Crime and London Chairman of the Federation of Small Businesses, with talks from Sophos and City of London Police, who are promoting Action Fraud and the law enforcement response to fraud in these	There is some progress against this recommendation: MOPAC is attempting to raise awareness about Action Fraud among businesses. However, MOPAC's response did not explain what it is doing to raise awareness among the public. And it not comment on whether it would use the Mayor to raise the profile of

Committee's recommendation	Response	Progress
individuals and businesses.	presentations through the LDSC. The LDSC is also actively engaged with Barclays and the Royal Bank of Scotland and presenting at their events for SMEs, and are promoting Action Fraud there too.	its campaign.
Recommendation 5: MOPAC should help Safer Neighbourhood Boards (SNBs) to raise awareness about online crime and the role of Action Fraud. It should provide SNBs with borough-level fraud and online crime statistics to help them to identify vulnerable groups in their area. To begin with, MOPAC should pilot events at meetings for two Safer Neighbourhood Boards. It should then collect findings from these meetings and feed these back to all other boards across London by the end of 2015-16.	MOPAC says it will take the activity of the LDSC to SNBs after its initial tranche of roadshows are complete later in 2015. LDSC will work on a programme of engagement on digital issues through the SNBs.	This recommendation has been substantially accepted: MOPAC intends to engage with SNBs as the Committee suggested.
Recommendation 6: To help the Met to avoid viewing cyber-crime in isolation, MOPAC should commit that its future strategies across all themes will directly address pertinent internet risks.	MOPAC says it is already considering how the digital environment can enable stalking and harrassment. These risks have been written into the Hate Crime Strategy. MOPAC ensures that all its strategies cover the online nature of crime and abuse.	This recommendation has been accepted.
Recommendation 7:	The Commissioner, in his formal response to the report, said	This recommendation has been substantially

Committee's recommendation	Response	Progress
Before the Met expands the FALCON command to phase three, it should assess whether it would be more beneficial to operate with a higher proportion of expert civilian staff relative to warranted officers.	that FALCON has embarked on a Police Staff Investigator programme to explore the Met's ability to recruit and retain non-warranted staff, enabling them to work alongside detectives to combat cyber-crime. Currently nine staff members are undertaking the programme.	accepted: the Met recognises that civilian staff, as well as, police officers will be an important resource to help tackle online theft and fraud.
Recommendation 8: MOPAC should develop and publish an online crime performance dashboard on a quarterly basis from 2016-17 onwards. Once the data is available, the dashboard should include the headline levels of online victimisation reported in its public and business attitudes surveys. The dashboard should also include the number of referrals that the Met receives through Action Fraud, as well as the proportion of positive and negative outcomes. And it should include suitable performance indicators that demonstrate the work that the Met is doing to prevent online crime and disrupt cyber-criminals.	In its response, MOPAC stated that it already hears about the impact of fraud on businesses through its Business Crime Change Board which the Deputy Mayor for Policing and Crime chairs jointly with the Deputy Commissioner, including the number of positive outcomes of National Fraud Investigation Bureau referrals from Operation Falcon. MOPAC is launching a fraud dashboard after the July Business Crime Change Board. This is about positive outcomes of fraud reports from Action Fraud.	This recommendation has been accepted in part: MOPAC says it is launching a fraud dashboard.
Recommendation 9: The Met should identify a senior	The Commissioner, in his formal response to the report, stated that he has appointed Commander Duncan Ball to be	This recommendation has been accepted in full.

Committee's recommendation	Response	Progress
ranking officer (ACPO level), to be responsible for mainstreaming cyber-crime across the whole of the force.	the ACPO lead for mainstreaming cyber-crime across the Met.	
Recommendation 10 In August 2015, once the FALCON command has been operating for a year, the Met should extend FALCON's buddying system outside of the command. For example, police officers and staff based in borough teams could be buddied with those based in FALCON's Volume Fraud Teams.	The Commissioner, in his formal response to the report, explained that the Met has taken steps to establish informal support outside of the command, including a formalised support mechanism between FALCON Volume Fraud Teams and borough teams. This will include "investigation surgeries" where advice on specific enquiries outside of FALCON's remit can be sought. The response did not include a specific commitment to introduce a buddying system, however.	This recommendation has been accepted in part: the Met is taking some steps to help to integrate the FALCON command with the rest of the organisation.
Recommendation 11 The Met should set a deadline for when it wants all staff with public contact and/or investigative duties to have undertaken the cyber-crime e-learning programme. It should also assess whether it needs to extend Mainstream Cyber-Crime training to officers and staff outside of the FALCON command and, if so, by when.	The Commissioner, in his formal response to the report, stated that the Met expects all staff that have contact with the public and/or investigative duties to have undertaken relevant cyber-crime training.	This recommendation has been accepted.