are working with ROCU to provide guidance to officers who have to investigate such offences, with the force lead being Detective Inspector DPA (OCSET). The guidance has been prepared and is currently waiting for senior leadership approval. It is recognised that there are many intelligence gaps around the motivation and activity of these individuals. Their actions carry the following risks; issues such as potentially undermining law enforcement activity, accidental exposure of individuals who are not involved in CSE and proper consideration to victim care. There is also a considerable suicide risk associated with this type of offending. A vigilante working in isolation of the police may not consider this risk. (See Paragraph 260 below).

71. An emerging trend appeared in 2015 across the West Midlands Region whereby victims were contacted by offenders via messaging apps such as 'Skype' and 'Oovoo'. The offenders would actively search for the victims and then befriend them. They would engage in conversation over the various social platforms and encourage them to remove their clothing and make sexually suggestive poses or engage in masturbation whilst on camera. The offenders record or take a screen capture of the victim and use the imagery to blackmail them. Offenders proceed to blackmail the victims by making threats of publishing the video or image onto Facebook and share it with all the victim's friends and family unless they continue to perform sexual acts for them or give them money. This type of offending is demonstrated at *Point 8iii (*example 1 paragraphs 106 to 116 below). The most recent method of offending (MO), which the NCA have been made aware of, relates to victims being blackmailed into making payments to offenders via Bitcoin. Bitcoin is a securely encrypted digital asset payment system which is used by people and businesses to transfer funds.

72. *Point 6iii) any distinguishing characteristics or trends in online child sexual abuse perpetrated by children and young people in your force area;*

73. I have already highlighted the rising trend in 'sexting' and peer to peer type offending at paragraphs 64 and 65 above and the way in which WMP are taking a proportionate response in order to deal with it.

74. The search of WMP Discoverer crime data base using the criteria as detailed at paragraph 58 revealed age characteristics of the victims. Between 2012 and September 2017 there has been a steady and almost equal rise in reported incidents in all age categories, 10-12, 13-15 and 16-17 years. The age category 13- 15 years is by far the largest group of victims accounting for between 50 and 60 per cent of all the reported internet associated crimes.

75. *Point 7. As regards scale, all relevant information and data including all relevant and available statistics or estimates from as far back in time as possible, including;*

Point 7i) the number of referrals made to the force by NCA-CEOP;

vulnerable victims and identify intelligence led opportunities for enforcement activity against offenders.

91. Data with regards to the time taken to deal with such referrals is collated within OCSET and can be ascertained from 2013 as follows;

Year	No. CEOP Referrals	Average	Shortest	Longest
2013 (Jan to Dec)	161	5	1	46
2014 (Jan to Dec)	107	2	1	18
2015 (Jan to Dec)	190	3	1	43
2016 (Jan to Dec)	205	3	1	41
2017 (Jan to Sep)	242	2	1	76

92. *Point 8ii. The use of the Child Abuse Image Database;*

93. The identification of victims of online abuse is a specialist investigative function which is carried out by the trained investigators within OCSET. The primary roles of the investigators when investigating offences of online child exploitation is the identification of victims, offenders and the locations where child abuse is being perpetrated. To be clear, victim Identification within WMP is not the responsibility of one Force officer but is the responsibility of any officer dealing with indecent images of children (IIOC) cases.

94. The Child Abuse Image Database (CAID) is used by the Force to assist in the identification of victims, offenders and locations and avoids duplicity across investigations. Within WMP OCSET the specialised team has been trained on CAID and have individual access. This enables each officer to interrogate the CAID database and where new images are found they will liaise with staff from the force Digital Forensic department, who are responsible for the administration of the system.

95. WMP Digital Forensics department receive exhibits (computers, memory sticks, mobile phones) to examine and establish if there is any IIOC material or evidence/ intelligence of online child sexual abuse. As system administrators the staff at Digital Forensics are responsible for uploading any newly identified first generation IIOC onto CAID. This will be material that has been identified from exhibits that they have examined or material notified to them by OCSET investigators.

96. WMP Digital Forensics department is in the process of completing the ISO/IEC 17025 accreditation and as part of that process they use a number of Standard Operating