Witness Statement
(CJ Act 1967, s.9; MC Act 1980, ss.5A(3) (a) and 5B; Criminal Procedure Rules 2015, Rule 27.1)

Statement of Stephen Harry Cordon – IF/7843/15   Page No. 1

Age if under 18.... over 18 (if over 18 insert 'over 18').

This statement (consisting of 4 pages each signed by me) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

Dated the 18th May 2015

Signature: **Signature**

I am employed by IntaForensics as a Computer Forensic Analyst. I obtained a First Class BSc (Hons) Forensic Computing degree at De Montfort University. I have previously worked for Palmer Legal Technologies as a Computer Forensic Associate. Alongside my degree I have received expert witness training in Excellence in Written Evidence and Witness Familiarisation from Bond Solon. I have completed training in the forensic acquisition and analysis tool Encase from Guidance Software to an advanced level and also received accreditation as an EnCase Certified Examiner (EnCE), which is awarded by Guidance Software. I have completed the IntaForensics peer assessed module on the procedural requirements of exhibit continuity and Forensic Imaging of digital media.

In this statement I shall, of my own accord, endeavour to restrict myself to matters that I believe to be factual and when proffering an opinion, will clearly indicate it as such. Throughout my analysis I made contemporaneous notes that report my practices and findings, in both handwritten and electronic form, these are retained in secure storage at my place of work and may be disclosed later if required.

All forensic examinations were conducted in accordance with **Association of Chief Police Officers (ACPO)** Good Practice Guide for Digital Evidence.

IntaForensics have been instructed by **David Parish** of **The Metropolitan Police**, to conduct a Forensic Analysis of the electronic data contained on exhibits **BSG/09** and **RLB/01**; in relation to Metropolitan Police Laboratory reference **CSL/0664/15** (IntaForensics case reference IF/7843/15) at the **Nuneaton** laboratory.

Signature ... **Signature** ....

One (1) USB Device has been produced containing Generated Materials referred to in this Witness Statement; this is now produced as exhibit **SHC/1**, in sealed exhibit bag, number **MPSA20172117.**

Exhibit **SHC/1** is now produced in **Transit Bag** seal number **TG0035589.**

The hard drive removed from exhibit **BSG/09** (hereafter referred to as **BSG/09/H1**) was found to contain the Operating System **Windows 7 Home Premium** was identified as being installed on the exhibit **BSG/09/H1** and is reported to have been installed on the **13th January 2011** at **15:30.** The Operating System Install Date is the date the current Operating System was installed relative to the computer system clock at the time of installation. **One (1)** non-default user account was identified on the exhibit **BSG/09/H1** with the user name **"Ben", "Stephen",** "[Name Redacted]" and "[Name Redacted]". The user accounts **"Ben"** and **"Stephen"** were found to be password protected therefore knowledge of this password is required to gain access to these computer user accounts. The passwords were of sufficient length/complexity that they could not be identified at the time of examination. It is not possible to determine if the user accounts "[Name Redacted]" and "[Name Redacted]" were password protected.

A review of files and communications stored on the exhibit **BSG/09/H1** was carried out using the software **EnCase version 6.19.7.2** and **Internet Evidence Finder version 6.5.1.0698.**

All user documents, images and movies stored on the exhibit **BSG/09/H1** have been extracted and produced for further review by the investigating officer. Reports containing the extracted data has now been produced as part of **SHC/1** in the folder **"BSG-09-H1"**. These reports are named after their content for example all extracted images from exhibit **BSG/09/H1** can be viewed by accessing the report **"BSG-09-H1\Images\BSG-09-H1 Images.html".**

One (1) iPhone Backup was identified on the exhibit **BSG/09/H1**. This backup was of an **iPhone 4** with the owner name "[Name Redacted]**'s iPhone**" and the phone number "[DPA]**282**". All data including stored images, contacts and text messages has been extracted from this backup using the software **XRY v6.13**. A report has been produced containing this information. This is now produced as part of **SHC/1** as the file **"BSG-09-H1\iPhone Backup**[Name Redacted]**s iPhone Backup Report.html"** for further review by the investigating officer.

Signature . **Signature**