Prosecuting Cyber-enabled Crime - A Case Study

Benjamin Lim

University of Edinburgh

s2599925@ed.ac.uk

April 5, 2025

1. Introduction

Ramon Abbas, also known as Ray Hushpuppi on Instagram, was arrested for fraud and money laundering in 2020. These offences are commonly categorized as cyber-enabled crimes, where technology is used as a tool to facilitate "traditional forms of crime" [1] [2]. Straddling the cyber-physical boundary, such crimes pose challenges to investigators as they have to rely on digital evidence to prosecute the perpetrator under various laws such as the Fraud Act (FA) [3], the Proceeds of Crime Act (PoCA) [4] and the Computer Misuse Act (CMA) [5].

In the following paragraphs, we would explore how Business Email Compromise (BEC) works and highlight various lines of investigations to attempt tracing the source Internet Protocol (IP) address behind the crime. Then, we will look at the technical and legal challenges of collecting the evidence in a forensically sound manner and analyzing it to determine the identity of the perpetrator. We will then shift to exploring the Placement, Layering and Integration stages of Money Laundering and the various regulations in place to detect such activity. Finally, we will look at jurisdictional issues if the perpetrator is overseas and explore legal instruments that can overcome these issues. Throughout the essay, we will be using court documents to examine how Abbas executed these crimes.

2. Business Email Compromise

BEC compromises two separate actions. The first involves gaining unauthorized access to the victim's email account usually by various means such as social engineering the victim to reveal their password or by brute forcing weak passwords [6]. Once access has been gained, the perpetrator will monitor inbound emails for an indeterminate period of time, waiting for an opportunity to strike. A possible opportunity could be the closure of a business deal or in Abbas's case, the refinance of a property [7]. For the second action, the perpetrator will interject and provide the bank account information of a money mule hoping to divert the payment into that ac-

1 Eric Rutger Leukfeldt, RJ Notté, and M Malsch, 'Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes' [2019] Victims & Offenders <https://doi.org/10.1080/15564886.2019.1672229>, pp. 1

2 Eoghan Casey, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet* (3rd, 2011), pp. 40

3 Fraud Act 2006

4 Proceeds of Crime Act 2002

5 Computer Misuse Act 1990

6 Cassandra Cross and Rosalie Gillett, 'Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud' (2020) 27(3) Journal of Financial Crime 871, pp. 873

7 United States District Court for the Central District of California, *Complaint filed as to Defendant Ramon Olorunwa Abbas in violation of 18:1956(h).* (2020) <https://storage.courtlistener.com/recap/gov.uscourts.cacd.790162/gov.uscourts.cacd.790162.1.0_1.pdf>, pp. 16

count [8] [9]. In Abbas's case, they compromised a law firm's email account, observed the pending deal, and sent a "spoofed" email to that law firm masquerading as Citizens Bank to arrange the loan payment to be sent to a Chase account [10]. The BEC concludes once the victim law firm sends the payment to the money mule's account.

The first action contravenes Section 2 of the CMA, as the perpetrator has gained "unauthorized access" to the victim's email account "with intent to commit or facilitate commission of a further offence" [11]. The further offence was committed through the second action, which contravenes Section 2 of the FA as the perpetrator made a "false representation" by masquerading as another party with the intention of "mak[ing] a gain for himself" through redirecting the transfer of funds to an account of his choosing [12].

3. Cyber Forensic investigation of BEC

As it's namesake suggests, investigation of BEC centres around email forensics. Once the crime has been discovered, the first step taken is to place a "litigation hold" on the email account [13] so that law enforcement can retrieve the email that the perpetrator sent in a forensically sound manner for further analysis [14]. The email header will contain the sender address and the source IP address from which the email was sent [15]. The perpetrator has two options here. They can spoof the domain by registering a similar domain such as citizenbank.com [16], and send out a legitimate email from that domain, hoping that the recipient would overlook the fact that the legitimate domain should have been citizensbank.com. This occurred in Naseeb v Director of Public Prosecutions (Naseeb) in which the perpetrator registered a domain felixohare.com which "had nothing to do with the construction company Felix O'Hare" [17]. They could also, as in Abbas's case, spoof the email directly [18]. While the latter method provides a more *prima facie* convincing email, email security features such as SPF and DKIM will likely cause the email to end up as spam or even get rejected outright [19]. Regardless of the method used, retrieving the email is often straightforward because the victim cooperates with law enforcement to provide the required evidence. The perpetrator might attempt to delete the email from the compromised inbox but copies can be obtained from the mail server since most organizations have an email retention policy that preserves permanently deleted emails for a period

8 Cross and Gillett (n 6), pp. 873

9 Graeme Edwards, *Cybercrime Investigators Handbook* (1st, 2019), pp. 23

10 United States District Court for the Central District of California (n 7), pp. 16

11 Computer Misuse Act 1990, Sect. 2

12 Fraud Act 2006, Sect. 2

13 Edwards (n 9), pp. 185

14 Reddy Niranjan, *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations* (1st, 2019), pp. 367-368

15 Casey (n 2), pp. 699

16 Cross and Gillett (n 6), pp. 873

17 *Naseeb v Director of Public Prosecutions* [2024] IEHC 37, para. 8 and 10

18 United States District Court for the Central District of California (n 7), pp. 16

19 DMARCLY, 'How to Implement DMARC/DKIM/SPF to Stop Email Spoofing/Phishing: The Definitive Guide' (20 February 2024) <https://dmarcly.com/blog/how-to-implement-dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide> accessed 25 January 2025

of time [20]. Rule 8 of the SRA Financial Services (Conduct of Business) Rules requires solicitors practicing in regulated financial activities to keep records for at least six years [21], and would have applied if the case occurred in the UK.

Once the source IP has been retrieved, it can be traced back to the perpetrator [22]. The IP could belong to a cloud provider, a Virtual Private Network (VPN) service or an Internet Service Provider (ISP). A witness summons or subpoena can be served on the service provider to reveal the identity of the person renting or subscribing to the service [23]. However, this step is usually challenging especially if the source IP is of foreign origin [24]. In a threat report, Mandiant was able to find out the attacker's IP address, email address and a possible birth year [25]. However, tracking the online persona to a "real world identity" is difficult due to lack of cooperation from the local authorities, especially if the state is suspected to be supporting the attack. Even without state support, there exist "Bulletproof Hosting" providers which set up shop in jurisdictions with lax laws and poor records of cooperation [26], advertising their non-compliance with law enforcement as a selling point.

4. BEC - Additional lines of investigations

Apart from email forensics, it would also be prudent to pursue additional lines of investigation by analyzing the compromised law firm's email account. Authentication logs would reveal if there were any sign-ins from an unknown IP address which can then be investigated in the same manner described above [27]. If no suspicious attempts were detected, then the computer which the victim staff used would be the next step. This is because the perpetrator could have planted a Remote Access Trojan (RAT) on that computer and accessed the email remotely via that computer [28]. If found, the RAT could be analyzed to determine the IP address issuing commands.

Another possible line of investigation would be to lodge a witness summons against the bank to retrieve the IP address, web browser version and operating system [29] which was used to login to the money mule's account. This avenue proved most useful in R v Khan, as the IP address was "used exclusively" at an address linked to the fraudster [30]. However, it must be noted that this can be easily circumvented through the use of a Virtual Private Network (VPN) as noted

20 Peter Sommer, *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers* (2012) <https://cryptome.org/2014/03/digital-investigations.pdf>, pp. 56

21 Solicitors Regulation Authority Board, *SRA Financial Services (Conduct of Business) Rules* (2018) <https://www.sra.org.uk/solicitors/standards-regulations/financial-services-conduct-business-rules/>

22 Niranjan (n 14), pp. 370

23 Edwards (n 9), pp. 185

24 Edwards (n 9), pp. 186

25 Mandiant, *APT1 - Exposing One of China's Cyber Espionage Units* (2021) <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>, pp. 58

26 Intel 471, 'Bulletproof Hosting: A Critical Cybercriminal Service' (24 January 2024) <https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service> accessed 25 January 2025

27 Edwards (n 9), pp. 38

28 Niranjan (n 14), pp. 278

29 National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (2006) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>, sect. 7.2.2

30 *R v Khan (Khawar)* [2011] EWCA Crim 1234, para. 10

31 *Naseeb v Director of Public Prosecutions* (n 17), para. 52

by the court in Naseeb's case [31]. The importance of obtaining the perpetrator's actual IP address cannot be understated. Nasseb's case was dismissed solely due to the lack of that critical piece of evidence [32].

Legislators are clearly aware of the ease of hiding one's tracks in cyberspace, hence the Investigatory Powers Act (IPA) 2016 was recently passed to empower law enforcement in collecting evidence for prosecuting serious crime [33]. The IPA *inter alia* allows law enforcement to mandate communications service providers to retain Internet Connection Records (ICR) of known suspects for up to 12 months[34]. ICR includes network traffic metadata such as the origin and destination IP address and port [35]. In our previous spoofed domain example, if we were able to capture network traffic metadata for citizenbank.com's mail server, any connections to the IMAP, POP3 or web ports would almost definitively be from the perpetrator's attempt to check for new emails [36], thus revealing his IP address. Koops asserts that such "legal hacking legislation" must adhere to the "minimum safeguards and requirements" in human rights case law [37]. Stoykova conjectures that should such measures be undertaken, law enforcement have may a duty to explain the use of "decryption methods and tools" and even "potentially [provide Digital Forensics] assistance" to the suspect [38]. Thus far, the IPA has not been challenged and its *de jure* legitimacy and effectiveness is yet to be proven.

5. Seizing Evidence

Once the IP address has been correlated to a real world identity, law enforcement can move ahead with the case. Assuming that the subject is based in the UK, an application for a search warrant must be lodged under the grounds that the IP address assigned to that person has been associated with fraud activities [39]. The Police and Criminal Evidence Act (PaCE) allows law enforcement to legally enter the premises and "seize anything" that may be "evidence in relation to an offence" [40]. This procedure was followed in R v Khan and law enforcement was able to seize incriminating evidence such as "credit card readers" and "driving licenses in various names" from the search warrant [41]. Apart from routers in residential addresses, cellular phones are also assigned IP addresses. Since phones are usually personal devices, it is extremely likely that the subscriber himself is the perpetrator. However, complications arise when residential addresses are occupied by a number of housemates, Stoykova explains that "necessity" and

32 *Naseeb v Director of Public Prosecutions* (n 17), para. 54

33 Investigatory Powers Act 2016

34 Investigatory Powers Act 2016, part. 4

35 NetQuest, 'The Reason Internet Connection Records are Valuable to Governments' (1 January 2024) <https://netquestcorp.com/internet-connection-records/> accessed 4 February 2025

36 Niranjan (n 14), pp. 347

37 Bert-Jaap Koops and Eleni Kosta, 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"' (2018) 34(4) Computer Law & Security Review 890 <https://www.sciencedirect.com/science/article/pii/S0267364918302413>, pp. 899

38 Radina Stoykova, 'Digital evidence: Unaddressed threats to fairness and the presumption of innocence' (2021) 42 Computer Law & Security Review 105575 <https://www.sciencedirect.com/science/article/pii/S0267364921000480>, pp. 6

39 Government Digital Service, *Code of practice for searches of premises by police officers And the seizure of property found by police officers On persons or premises* (2013) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903811/pace-code-b-2013.pdf>, pp. 9

40 Police and Criminal Evidence Act 1984, sect. 16 and 19

41 *R v Khan (Khawar)* (n 30), para. 11

"proportionality" tests may need to be undertaken to avoid infringing the rights of "groups of people", in this case, all the housemates [42]. At this juncture, the benefits of pursuing multiple lines of investigation reveal itself. Law enforcement may have additional information such as the operating system used by the perpetrator which might prove useful in narrowing down the list of suspects using devices from certain manufacturers and protecting the rights of innocent housemates. Such information could have been gleaned from the "User Agent" used when logging onto the victim's webmail server [43].

While executing the search warrant, law enforcement should immediately request the suspect to provide all passwords and pin codes to unlock the devices [44]. Some devices may be encrypted with the password as a key, hence it is crucial to obtain and verify the passwords before turning the device off or before it runs out of battery [45]. It is also good practice to attempt to preserve volatile evidence such as unsaved documents and clear text passwords which reside only in Random Access Memory (RAM) while the device is still powered on [46]. This can be achieved by running a portable executable off a USB drive which dumps the contents of the RAM onto a file in that same drive [47]. The use of a USB drive minimizes the volume of data written to the computer's disk drive, which reduces the probability of overwriting deleted data of interest [48]. This process can be complicated for law enforcement officers without a technical background, hence law enforcement officers can also put the computer in hibernation mode, which will preserve the contents of the RAM directly on the disk [49]. Hibernation is a simpler alternative with less probability of error, albeit at the expense of possibly overriding some deleted data of interest. Regardless of the method chosen, it is important to "make contemporaneous notes" of actions taken so it can be recounted in a witness statement later when questioned on possible contamination of the evidence [50].

For uncooperative suspects, the ideal scenario would be to leave the devices switched on, remove the Subscriber Identity Module (SIM) card for mobile phones and place the device in a Faraday bag [51]. A Faraday bag blocks electromagnetic waves and will prevent devices from being accessed wirelessly while the removal of the SIM card prevents any further connection to the cellular network [52], hence preventing the device from being wiped remotely. There have been incidents of devices being wiped remotely while in police custody [53]. In one particular case, witnesses had to be called to testify because the evidence had been wiped [54]. Accord-

42 Stoykova (n 38), pp. 7

43 National Institute of Standards and Technology (n 29), sect. 7.2.2

44 Edwards (n 9), pp. 111

45 Edwards (n 9), pp. 111

46 Niranjan (n 14), pp. 30

47 Casey (n 2), pp. 399

48 National Institute of Standards and Technology (n 29), sect. 5.2.1.1

49 Azad Singh, Pankaj Sharma, and Rajender Nath, 'Role of Hibernation File in Memory Forensics of windows 10' (2016) 7(12) International Journal of Scientific & Engineering Research 42, pp. 42

50 Sommer (n 20), pp. 48

51 Edwards (n 9), pp. 59

52 Edwards (n 9), pp. 59

53 Jane Wakefield, 'Devices being remotely wiped in police custody' (9 October 2014) <https://www.bbc.com/news/technology-29464889> accessed 31 January 2025

54 Louisa Tang, 'O-Level exam cheating case: Invigilators describe how cheating was discovered' (3 August 2018) <https://www.todayonline.com/singapore/o-level-exam-cheating-case-invigilators-describe-how-cheating-was-discovered> accessed 31 January 2025

ing to Smith, information "recorded by mechanical means without the intervention of a human mind" constitutes real evidence [55]. Real evidence carries greater weight than a witness testimony [56], hence the loss of that evidence could have resulted in an adverse outcome for the prosecution. After all the above steps have been taken to preserve as much evidence as possible, the seized electronic devices and storage devices should be placed in an evidence bag and sealed, so as to preserve the chain of custody (CoC) [57]. While the evidence is transported, any officer handling the evidence has to update the CoC document. When it is finally before the forensic examiner, the integrity of the seal has to be verified, this ensures that the evidence has not been tampered with during the journey from the crime scene to the forensic lab [58].

6. Analyzing Evidence

Back in the forensic lab, the first order of business is to make a forensically sound copy of all storage medium [59]. During this process, a physical write blocker should be used to prevent the possibility of modifying any data on the storage medium [60]. A hash of the image should be produced by the imaging tool while making the copy. Once completed, the evidence should be resealed and stored securely [61]. This procedure is required because as demonstrated in Einarsson v Iceland, the defendant can submit a request for "all data seized and held" [62], as denial of that data could possibly infringe the defendant's right to "preparation of his defense" under Article 6 of the European Convention on Human Rights (ECHR) [63]. In the Einarsson case, the judge dismissed his application as the data also included that of "great many customers of [the bank]" [64]. However, in our hypothetical example of seizing a BEC suspect's personal devices, that may not be the case. Thus, since the original storage medium may need to be presented to the defendant during the e-discovery process [65], it is crucial that the storage medium was never modified after seizure and that the analysis was performed on an identical copy with a matching hash. This allows the defendant to replicate the analysis, thus validating the findings of the forensic analyst.

With cyber-enabled crime, the approach is usually to perform a keyword search on all storage media. Law enforcement should have gathered a list of keywords which include the victim's email address, the money mule's bank account number and the spoofed domain. As demonstrated in the Enron case study [66], the analysis software will search though emails, documents and messages. Analysts would then have to look through those artefacts to determine if they are relevant to the case. For example, a copy of the spoofed email, communication with collaborators or money mules, bank statements or screenshots showing the transferred amount

55 John Cyril Smith, 'The admissibility of Statements by Computer' [1981] Criminal Law Review 390, pp. 396

56 Adrian Keane and Paul McKeown, *The Modern Law of Evidence* (9th, 2012), pp. 267

57 Edwards (n 9), pp. 56

58 Edwards (n 9), pp. 58

59 Edwards (n 9), pp. 62

60 National Institute of Standards and Technology (n 29), sect. 4.2.2

61 Sommer (n 20), pp. 49

62 *Case of Sigurdur Einarsson and Others V Iceland* [2019] ECHR 39757/15, para. 15

63 Convention for the Protection of Human Rights and Fundamental Freedoms ECtHR, (adopted 10 December 1948) (ECHR), art. 6

64 *Case of Sigurdur Einarsson and Others V Iceland* (n 62), para. 25

65 Sommer (n 20), pp. 85

66 Niranjan (n 14), pp. 374

would prove the suspect's guilt. In Abbas's case, law enforcement found messages between Abbas and coconspirators discussing the transfer as well as screenshots of the bank account used in the fraud [67]. During the analysis, it is common to uncover additional keywords such as coconspirators's phone number. Law enforcement would feed these keywords into the analysis software to uncover further documents which may reveal the coconspirators's identity. In Abbas's case, Coconspirator 1 was arrested on 17 October 2019 [68]. Subsequently, law enforcement found Abbas's number stored in his iPhone with the contact name "Hush" [69]. A Western Union money transfer with Abbas's phone number as the sender was found which linked Abbas to the case and likely resulted in his subsequent arrest [70]. This illustrates the importance of further analyzing additional keywords obtained from the initial search.

7. Money Laundering

Fraud is almost always interconnected with Money Laundering as criminals need to process their ill gotten gains and make it spendable. Thus, this provides additional avenues for investigators to trace the crime back to the perpetrators. There are generally three steps in money laundering, Placement, where illegal proceeds enter the system, Layering, where money is transferred repeatedly to obfuscate its source and Integration, where the newly cleaned money is spent legally [71].

Demetis posits that Placement is the most critical stage in detection, as it occurs before the transactions are broken up and scattered [72]. This sentiment is corroborated by the criminal complaint document in Abbas's case in which his coconspirator repeatedly exchanged messages discussing the availability of an "open beneficiary account" to receive the initial transfer from the victim [73]. Monitoring systems would alert on anomalous transactions [74] such as a high value transaction with no precedent from UK to Mexico as perpetuated by a coconspirator in Abbas's case [75].

These transactions are manually reviewed and a Suspicious Activity Report (SAR) may be filed with the UK Financial Intelligence Unit (FIU) and forwarded to the prosecution [76] in accordance with Section 330 of the PoCA [77]. This proved effective in Shah & Anor v HSBC, where the bank account was frozen while the Metropolitan Police investigated the account holder for money laundering [78]. Apart from anomalies, authorities also single out transactions to high-risk countries with "strategic defi-

67 United States District Court for the Central District of California (n 7), pp. 17

68 United States District Court for the Central District of California (n 7), pp. 18

69 United States District Court for the Central District of California (n 7), pp. 4

70 United States District Court for the Central District of California (n 7), pp. 13

71 Dionysios S Demetis, 'Fighting money laundering with technology: A case study of Bank X in the UK' (2018) 105 Decision Support Systems 96 <https://www.sciencedirect.com/science/article/pii/S0167923617302178>, pp. 97

72 Demetis (n 71), pp. 97

73 United States District Court for the Central District of California (n 7), pp. 22-25

74 Demetis (n 71), pp. 97

75 United States District Court for the Central District of California (n 7), pp. 25

76 Demetis (n 71), pp. 97

77 Proceeds of Crime Act 2002

78 *Shah & Anor v HSBC Private Bank (UK) Ltd* [2012] EWHC 1283, para. 9 and 10

79 Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies [2016] OJ L254/1

ciencies" in anti-money laundering for enhanced scrutiny [79] as well as transactions bound for sanctioned countries and entities [80]. In the Bangladesh central bank heist, these measures foiled a transfer of over $951 million dollars as the recipient bank address contained the word "Jupiter" which matched the name of a sanctioned Iranian vessel and company [81].

Since identification documents (ID) are required to open a bank account, we avoid the difficult issue of tracing source IP addresses to real identities. In Abbas's case, he convinced a businessperson to open a bank account which was subsequently used to receive illicit funds which were partially channeled to a luxury watch seller and a coconspirator [82]. In the Bangladesh central bank heist, perpetrators allegedly deceived a businesswoman into receiving $20 million in stolen funds on the context of funding a business project [83]. The businesswoman was instructed to transfer part of the funds into her personal account and that of an acquaintance [84]. This demonstrates the process of Layering where repeated transfers are performed to mask the source of the funds. In Abbas's case, the funds were used to purchase a luxury watch which represents a store of value. That said, Abbas's email contained documents of 13 different individuals with varying nationalities [85]. Thus, it is possible that fake or stolen IDs were used to open these bank accounts and further detective work may be required to unravel the identity of the perpetrator.

In the final stage of Integration, the perpetrator would be able to gain access to funds legitimately. In Abbas's case, he arranged for coconspirators to pick up the watch in the US and have it transported through a flight to the UAE [86] where the luxury watch might be sold to an unsuspecting buyer, leaving Abbas with cash and a receipt that explains the source of funds. In the Bangladesh central bank heist, the perpetrators used a casino in the Philippines as the final stop [87] where the money could be legitimately withdrawn as winnings after a few games of cards. In the UK, Money Service Businesses will need to keep customer records and file SARs, which assists detection when perpetrators attempt to fence illegally obtained luxury watches [88]. The PoCA is also binding on gambling operators in the UK, which must report instances of "known or suspected money laundering" [89]. Nonetheless, as we have witnessed in cases above, it is trivial for perpetrators to forum shop and select a jurisdiction with relaxed regulations, which we will address in the next

80 Financial Action Task Force, '"Black and grey" lists' (25 October 2024) <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html> accessed 25 February 2025

81 Shihar Aneez Seragul Quadir and others, 'The Bangladesh Bank Heist' (21 July 2017) <https://2017.sopawards.com/wp-content/uploads/2017/03/The-Bangladesh-Bank-Heist.pdf> accessed 25 February 2025, pp. 6

82 United States Attorney's Office for the Central District of California, *Plea Agreement for Defendant Ramon Olorunwa Abbas* (2021) <https://saharareporters.com/sites/default/files/gov.uscourts.cacd_790162.46.0-4.pdf>, pp. 15-16

83 Seragul Quadir and others (n 81), pp. 4

84 Seragul Quadir and others (n 81), pp. 4

85 United States District Court for the Central District of California (n 7), pp. 13

86 United States Attorney's Office for the Central District of California (n 82), pp. 16

87 Seragul Quadir and others (n 81), pp. 12

88 HM Revenue & Customs, *Anti-Money Laundering Supervision: Money Service Businesses* (2014) <https://assets.publishing.service.gov.uk/media/65c209f0688c39000d334bfa/Anti-Money_Laundering_Guidance_for_Money_Service_Businesses_240131.odt>, pp. 10-12

89 Gambling Commission, *Duties and responsibilities under the Proceeds of Crime Act 2002* (2020) <https://assets.ctfassets.net/j16ev64qyf6l/6QuVw2XGPlXepcm3h5UyHC/eee37f7f2d0967798a165be9643b63cb/Duties_and_responsibilities_under_POCA_4th_Ed_Rev_1__Clean_version_.pdf>, para 3.2 and 3.3

paragraph.

8. Jurisdiction and Territoriality

Regardless of the method used to obtain the perpetrator's identity, the next step is use the collected evidence to build a case and to bring the perpetrator into custody. If the perpetrator is based in the UK, the process is trivial. The case will be brought before the public prosecutor for approval after which a warrant is issued for the perpetrator's arrest [90].

However, if the perpetrator is based overseas, the principle of territoriality would come into play. For criminal activity, the "universality principle" is most appropriate as "all states [do share] a common or universal interest in [the] suppression" of these criminal activity [91]. The UK FIU has requested for and disseminated over a thousand intelligence reports to overseas FIUs in 2020 [92]. These intelligence sharing and collaboration does result in tangible outcomes. The UK is one of forty countries that participated in Operation HAECHI V spearheaded by The International Criminal Police Organization (INTERPOL), which resulted in the seizure of USD 400 million and the arrests of 5,500 criminals engaging in *inter alia* BEC fraud [93]. Nevertheless, due to its vast membership, organizations like INTERPOL have been criticized for accepting requests that may be "politically motivated" such as charges by a government against a former ousted president [94]. There is an alternative in the form of Mutual Legal Assistance Treaties (MLAT) [95], these agreements are generally bilateral in nature and hence sidestep the political deadlock caused by having too many voices at the table. Operation Cronos was led by the UK National Crime Agency (NCA) and co-ordinated at the European level, leading to the arrest of criminals behind ransomware activity that were based out of a single country [96]. Abbas himself was arrested in the UAE through the joint effort of US and UAE law enforcement agencies [97]. When all else fails, yet another effective strategy is to arrest perpetrators once they have entered the country. A federal arrest warrant was issued for one of Abbas's coconspirator, and he was subsequently arrested in a US airport shortly after arriving [98].

Money Laundering is a tricky topic where the aforementioned "universality principle" may not apply since some countries depend on the inflow

90 The Criminal Procedure Rules 2011, part. 18

91 Diane Rowland, Uta Kohl, and Andrew Charlesworth, *Information Technology Law* (5th, 2016), pp. 43

92 National Crime Agency, *Suspicious Activity Reports Annual Report 2020* (2006) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file>, pp. 7

93 The International Criminal Police Organization, 'INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million' (27 November 2024) <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million> accessed 28 February 2025

94 Open Society Foundations, 'Is Interpol Vulnerable to Political Abuse?' (20 January 2015) <https://www.opensocietyfoundations.org/voices/interpol-vulnerable-political-abuse> accessed 2 March 2025

95 Home Office, *International MLA & extradition Agreements the UK is party to* (2023) <https://assets.publishing.service.gov.uk/media/64fad640fdc5d1000dfce80f/Treaty_List_August_2023.pdf>

96 Europol, 'Law enforcement disrupt world's biggest ransomware operation' (20 February 2024) <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation> accessed 2 March 2025

97 US Attorney's Office, Central District of California, 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams' (7 November 2022) <https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions> accessed 4 April 2025

98 United States District Court for the Central District of California (n 7), pp. 18

of illicit funds and thus may not be as willing to suppress these activities [99]. To keep the playing field equal, the Financial Action Task Force (FATF) maintains a grey list and a black list of countries [100], urging countries to apply "due dilligence" in checking transactions to countries on the list and in severe cases such as North Korea, recommending to terminate all banking activity [101]. Such measures exclude these non-compliant countries from the financial system, forcing criminals into cooperative jurisdictions where MLATs and INTERPOL are effective. Once an arrest is made by local law enforcement, they can then be extradited back to the country of origin to face a criminal trial in court.

9. Conclusion

Ramon Abbas is but one of many criminals engaging in BEC and subsequently money laundering the ill gotten gains. Using his case as an example, we have stepped through the process behind BEC, explaining how it is illegal under FA, PoCa and the CMA. We identified how emails, domains and mail servers can be used as a starting point in the investigation to determine the perpetrator's IP address. We then looked at attributing it to a real world identity and how digital evidence can be seized and analyzed with minimal risk of spoilation to support the case in court.

Next, we observed how Placement, Layering and Integration allows Abbas and the perpetrators behind the Bangladesh central bank heist to launder proceeds of crimes, and its illegality under PoCA. Since financial accounts, unlike most online activity, are tied to a real world identity, it gives law enforcement additional investigation opportunities.

Finally, we explored the various legal instruments available to law enforcement for cases that span multiple jurisdictions. Given the recent successes in joint operations tackling cyber-enabled crime, continued collaboration and improvement will ensure that future Abbases are brought to justice.

---

99 FATF, INTERPOL and Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud* (2023) <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>, pp. 14

100 Financial Action Task Force, '"Black and grey" lists' (n 80)

101 Financial Action Task Force, 'Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures' (21 February 2025) <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2025.html> accessed 2 March 2025

Bibliography

Cases

Case of Sigurdur Einarsson and Others V Iceland [2019] ECHR 39757/15.

Naseeb v Director of Public Prosecutions [2024] IEHC 37.

R v Khan (Khawar) [2011] EWCA Crim 1234.

Shah & Anor v HSBC Private Bank (UK) Ltd [2012] EWHC 1283.

Legislation

Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies [2016] OJ L254/1.

Computer Misuse Act 1990.

Fraud Act 2006.

Investigatory Powers Act 2016.

Police and Criminal Evidence Act 1984.

Proceeds of Crime Act 2002.

The Criminal Procedure Rules 2011.

Treaties

Convention for the Protection of Human Rights and Fundamental Freedoms ECtHR, (adopted 10 December 1948).

Reports

FATF, INTERPOL and Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud* (2023) <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>.

Gambling Commission, *Duties and responsibilities under the Proceeds of Crime Act 2002* (2020) <https://assets.ctfassets.net/j16ev64qyf6l/6QuVw2XGPlXepcm3h5UyHC/eee37f7f2d0967798a Duties_and_responsibilities_under_POCA_4th_Ed_Rev_1__Clean_version_.pdf>.

Government Digital Service, *Code of practice for searches of premises by police officers And the seizure of property found by police officers On persons or premises* (2013) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/903811/pace-code-b-2013.pdf>.

HM Revenue & Customs, *Anti-Money Laundering Supervision: Money Service Businesses* (2014) <https://assets.publishing.service.gov.uk/media/65c209f0688c39000d334bfa/Anti-Money_Laundering_Guidance_for_Money_Service_Businesses_240131.odt>.

Home Office, *International MLA & extradition Agreements the UK is party to* (2023) <https://assets.publishing.service.gov.uk/media/64fad640fdc5d1000dfce80f/Treaty_List_August_2023.pdf>.

Mandiant, *APT1 - Exposing One of China's Cyber Espionage Units* (2021) <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>.

National Crime Agency, *Suspicious Activity Reports Annual Report 2020* (2006) <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/480-sars-annual-report-2020/file>.

National Institute of Standards and Technology, *Guide to Integrating Forensic Techniques into Incident Response* (2006) <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800 86.pdf>.

Solicitors Regulation Authority Board, *SRA Financial Services (Conduct of Business) Rules* (2018) <https://www.sra.org.uk/solicitors/standards-regulations/financial-services-conduct-business-rules/>.

Sommer P, *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers* (2012) <https://cryptome.org/2014/03/digital-investigations.pdf>.

United States Attorney's Office for the Central District of California, *Plea Agreement for Defendant Ramon Olorunwa Abbas* (2021) <https://saharareporters.com/sites/default/files/gov.uscourts.cacd_790162.46.0-4.pdf>.

United States District Court for the Central District of California, *Complaint filed as to Defendant Ramon Olorunwa Abbas in violation of 18:1956(h).* (2020) <https://storage.courtlistener.com/recap/gov.uscourts.cacd.790162/gov.uscourts.cacd.790162.1.0_1.pdf>.

Books

Casey E, *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet* (3rd, 2011).

Edwards G, *Cybercrime Investigators Handbook* (1st, 2019).

Keane A and McKeown P, *The Modern Law of Evidence* (9th, 2012).

Niranjan R, *Practical Cyber Forensics: An Incident-Based Approach to Forensic Investigations* (1st, 2019).

Rowland D, Kohl U, and Charlesworth A, *Information Technology Law* (5th, 2016).

Articles

Cross C and Gillett R, 'Exploiting Trust for Financial Gain: An Overview of Business Email Compromise (BEC) Fraud' (2020) 27(3) Journal of Financial Crime 871.

Demetis DS, 'Fighting money laundering with technology: A case study of Bank X in the UK' (2018) 105 Decision Support Systems 96 <https://www.sciencedirect.com/science/article/pii/S0167923617302178>.

Koops B.-J and Kosta E, 'Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark"' (2018) 34(4) Computer Law & Security Review 890 <https://www.sciencedirect.com/science/article/pii/S0267364918302413>.

Leukfeldt ER, Notté RJ, and Malsch M, 'Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes' [2019] Victims & Offenders <https://doi.org/10.1080/15564886.2019.1672229>.

Singh A, Sharma P, and Nath R, 'Role of Hibernation File in Memory Forensics of windows 10' (2016) 7(12) International Journal of Scientific & Engineering Research 42.

Smith JC, 'The admissibility of Statements by Computer' [1981] Criminal Law Review 390.

Stoykova R, 'Digital evidence: Unaddressed threats to fairness and the presumption of innocence' (2021) 42 Computer Law & Security Review 105575 <https://www.sciencedirect.com/science/article/pii/S0267364921000480>.

Secondary Sources

DMARCLY, 'How to Implement DMARC/DKIM/SPF to Stop Email Spoofing/Phishing: The Definitive Guide' (20 February 2024) <https://dmarcly.com/blog/how-to-implement-

dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide> accessed 25 January 2025.

Europol, 'Law enforcement disrupt world's biggest ransomware operation' (20 February 2024) <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation> accessed 2 March 2025.

Financial Action Task Force, '"Black and grey" lists' (25 October 2024) <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html> accessed 25 February 2025.

— 'Jurisdictions subject to a FATF call on its members and other jurisdictions to apply countermeasures' (21 February 2025) <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2025.html> accessed 2 March 2025.

Intel 471, 'Bulletproof Hosting: A Critical Cybercriminal Service' (24 January 2024) <https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service> accessed 25 January 2025.

NetQuest, 'The Reason Internet Connection Records are Valuable to Governments' (1 January 2024) <https://netquestcorp.com/internet-connection-records/> accessed 4 February 2025.

Open Society Foundations, 'Is Interpol Vulnerable to Political Abuse?' (20 January 2015) <https://www.opensocietyfoundations.org/voices/interpol-vulnerable-political-abuse> accessed 2 March 2025.

Seragul Quadir SA and others, 'The Bangladesh Bank Heist' (21 July 2017) <https://2017.sopawards.com/wp-content/uploads/2017/03/The-Bangladesh-Bank-Heist.pdf> accessed 25 February 2025.

Tang L, 'O-Level exam cheating case: Invigilators describe how cheating was discovered' (3 August 2018) <https://www.todayonline.com/singapore/o-level-exam-cheating-case-invigilators-describe-how-cheating-was-discovered> accessed 31 January 2025.

The International Criminal Police Organization, 'INTERPOL financial crime operation makes record 5,500 arrests, seizures worth over USD 400 million' (27 November 2024) <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-financial-crime-operation-makes-record-5-500-arrests-seizures-worth-over-USD-400-million> accessed 28 February 2025.

US Attorney's Office, Central District of California, 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams' (7 November 2022) <https://www.justice.gov/usao-cdca/pr/nigerian-man-

sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions> accessed 4 April 2025.

Wakefield J, 'Devices being remotely wiped in police custody' (9 October 2014) <https://www.bbc.com/news/technology-29464889> accessed 31 January 2025.