An expert advisory report on the United Kingdom's approach to cyber identity theft.

December 2022

Contents

1 Introduction and background

Due to the surge in reported cyber identity theft cases and associated costs, this report aims to evaluate current measures to combat identity cybercrime and offer the UK Government considerations for future policy.

Cyber identity theft is defined as stealing credentials from potential victims, which could be used for intelligence gathering or identity fraud, whereby the goods or services are obtained by deception from the stolen identity (ENISA, 2020).

The National Cyber Force (NCF) set up in 2020 as part of the UK Government's National Cyber Strategy has been an effective measure to intervene in cyber identity theft with attempts to block online credit card fraud, the highest method of cyber fraud. However, with over 226,000 identity theft cases recorded in 2021 (Statista, 2022), an increase of 21%, the NCF has further challenges to overcome.

2 Cyber Identity Theft in the UK:

2.1 Manifestation

Cyber identity theft has manifested itself deeply in many sectors of society. Social media has facilitated the rise of identity theft by providing unique targeted victims for cybercriminals to exploit (Burnap et al., 2014), and Williams (2015) argues that social engineering methods such as phishing are the most popular for perpetrators, particularly in cultivated attacks such as pharming personal data, spear phishing and targeting specific people. Specifically, victims would be targeted using automatic directions to imitation false websites and SMS text message deceptions. Malware technologies whereby perpetrators log users' keystrokes to perform unauthorised actions to steal credentials and access financial information (Williams, 2015). Convenience and simplicity are available for cybercriminals, including predesigned packages readily available through masked identity on the dark web. However, law enforcement authorities are collaborating to challenge the largest underground criminal parties. National Economic Crime Centre, National Crime Agency, and Metropolitan Police all collaborated with international authorities in the US and Ukraine to arrest an international criminal group and arrest over 100 people in the UK (Metropolitan Police, 2022). Nonetheless, it should be noted that 16% of all referred cyber crimes in 2019-2021 (Action Fraud, 2021b) ended up in a judicial outcome and the trend deteriorated from 2020-2021 to 5% of judicial outcomes identifying phishing emails as the critical enabler for criminals (Action Fraud, 2021a).

The internal insider poses a threat to society. Online retailers have witnessed rapid growth in credit card use which has seen the highest rate of cyber-related fraud. From

2020-2021 retail e-commerce growth accelerated by 18.8% in the UK (Fisher and Perkins, 2022) and the opportunities for cyber-related crime trend accordingly. CIFAS UK's fraud prevention community organisation, reported in 2017 that the unlawful obtaining or disclosing of personal data increased by 29% from 2016 (CIFAS, 2017). Limitations in preventative measures introduced have facilitated this increase and greater emphasis on security frameworks, such as the Role-Based Framework (Okeke and Eiza, 2022), to place more accountability on management within companies to audit employees and acquire sufficient infrastructure policy. First-line management of detection and investigation with collaborative middle managers to adhere to deterrence policies, victim assistance, incident training, data compliance and partnership with law enforcement authorities could lead to potential prosecution.

2.2 Transnational ramifications

Transnationally, the nature of cybercrime does not need to be in physical neighbourhoods, with the internet providing no frontiers. Victimisation can vary significantly between nations depending on urbanicity and economic performance (Kesteren et al., 2014). The correlation between countries that did not sign the Council of Europe Convention on Cybercrime and those that have not implemented a successful strategy often harbour criminals due to policies without inter-jurisdictional and extradition protocol as they have a lessened risk of apprehension (Williams, 2015). In recent years, national law enforcement agencies, EUROPOL, and INTERPOL Threat Cybercrime Response Team have become tasked with managing ransomware attacks from anonymous criminals holding medical services and hospitals, placing a response on protecting critical infrastructure (Radoini, 2020). These efforts withdraw planning away from cyber identity theft crimes. Furthermore, extending a coordinated approach from the local to national level and collaboration with international authorities becomes complicated, requiring a significant investment of resources.

Whereby perpetrators are required to be surrendered by neighbouring European Union members, the European Arrest Warrant (EAW) can support this process; however, as yet, digital identity theft is not included as an offence but is recommended in the European Parliament resolution of 2021 (Official Journal of the European Union, 2021). The EAW should be used carefully, as in the case of Choudary v France (EWHC, 2020); the appellant was subject to identity theft and sentenced to three years in France in 2015. The French authorities requested an EAW for prosecution from the

UK to France. The verdict was mistaken identity and can indicate that law enforcement should carefully review case materials or the use of EAW can be questioned.

3 Considerations of rights and ethics

Any breach presents information disclosure of a subject's personal life and habits, potentially leading to material damage or risk to physical integrity. Cyber identity theft through social engineering serves as a high-risk rating by the European Data Protection Board (EDPB) established by the EU GDPR (Intersoft Consulting, N.D.) as a potential risk to the rights and freedoms of an individual. Under GDPR, the national supervisory authority should be contacted and communicate with the victim under Articles 33 and 34. To reduce future events, organisations that have been breached should use improved forms of authentication, such as multi-factor authentication (EDPB, 2021).

GDPR Articles 15-21 offer individuals the requested right to access their data; however, this can offer concerns when a person's identity has been stolen. The data controller may request additional information to confirm identity; nonetheless, authentication and identity verification processes should be evaluated (Sumner, 2017). Education and training of employees and organisations should have security protocols and controls in place so that individuals achieve Articles 15-21; however, measures are defined by GDPR, which places more significant preparation of policy on organisations.

Furthermore, it should be considered the impact of GDPR on the public and private sectors. The public sector body, Department for Education (DfE), was formally reprimanded for a severe breach of GDPR by the unauthorised sharing of 28 million children's data (Information Commissioner’s Office, 2022) under GDPR Article 5. There was no financial penalty for this as the payment would likely come from public funds; however, it raises the concern of consistency when private sector companies

are heavily financially fined for personal data breaches on a smaller scale. The UK government are considering a UK GDPR reform on the Data Protection and Digital Information Bill (Hasan, 2022) to facilitate trustworthy use of data. Transferring data transnationally would undergo determination that the standard of protection for a data subject must meet UK standards.

Considering cross-border data flow and fundamental rights, the judgement case of Big Brother Watch and Others v. the United Kingdom (Grand Chamber of the European Court of Human Rights, 2021), we understand that the UK Regulation of Investigatory Powers Act 2002 (RIPA) violated ECHR Article 8 the right to respect for private and family life due to bulk inception rules of material from devices for potential investigation. This act has now been replaced by the Investigatory Powers Act 2016 (IPA), which ensures Article 8 is not breached, although there are concerns about its protection. The ECHR has stated that bulk interception is not a violation of human rights due to the threats in modern society. Law enforcement will have the means to use this method for gaining data; however, they will face challenges in managing their protocols for receiving admissible evidence.

Further challenges may also come from the proposed Bill of Rights Bill (Raab, 2022), which will replace the Human Rights Act (HRA) 1998. Under the HRA, the UK parliament empowered British judges to protect rights contained in the ECHR. The court would declare incompatibility if legislation were to violate human rights. Under the Bill of Rights Bill, the violating legislation is not prevented from being enforced, with ministers passing a costly and lengthy remedial order to rectify it (Stevens and Marsons, 2022).

In recent years, Article 8 Human Rights Act (the right to private life) has influenced UK legislation, and resultant case law devised to combat cybersecurity issues. The advent

of Dominic Raab's proposed Bill of Rights (Raab, 2022) poses a threat to this. Domestic courts may no longer be bound by judgments or directives of the European Court of Human Rights (ECHR), and the Bill paves the way for British law to take supremacy. There are arguments that this could weaken human rights. The judiciary's ability to declare legislation incompatible with ECHR will likely be removed. It remains to be seen how these changes would take effect in practice, but there is a risk that a layer of protection could be displaced.

4 UK law effectiveness

Digital evidence in courts of law challenges existing legal procedures developed for traditional evidence types. Identity theft alone is not classified as a police recordable offence, according to the UK Home Office (World Association of Professional Investigators, 2021). Crime can only be recorded on behalf of the person or organisation that was defrauded due to the misuse of identity. For a crime to be committed for law enforcement, reports are made to Action Fraud, which transfers information to the National Fraud Intelligence Bureau (NFIB) to decide after investigation assessment.

The legal framework offers numerous Acts of Parliament (Figure 1) to cover five investigative areas (Goldstraw-White, 2022).

Data Extraction	Data Review	Disclosure	Presentation	Privacy
• Investigatory Powers Act 2016 • Police, Crime, Sentencing and Courts Act 2022 (only part in force) • Police Act 1997 • Police and Criminal Evidence Act (PACE) 1984 • Policing and Crime Act 2017 • Regulation of Investigatory Powers Act (RIPA) 2000 • Data Protection Act 2018 • Criminal Procedures and Investigations Act 1996 • Criminal Justice and Police Act 2001 • Human Rights Act 1998 • Computer Misuse Act 1990 • Serious Crime Act 2015	• Computer Misuse Act 1990 • Regulation of Investigatory Powers Act (RIPA) 2000 • Police and Criminal Evidence Act (PACE) 1984 • Data Protection Act 2018 • Electronic Communications Act 2000 • Criminal Justice and Police Act 2001 • Investigatory Powers Act 2016	• Criminal Procedures and Investigations Act 1996 • Data Protection Act 2018	• Police and Criminal Evidence Act (PACE) 1984 • Criminal Justice Act 2003 • Electronic Communications Act 2000 • Criminal Procedures and Investigations Act 1996 • Data Protection Act 2018	• Regulation of Investigatory Powers Act (RIPA) 2000 • Data Protection Act 2018 • Criminal Procedures and Investigations Act 1996 • Criminal Justice and Police Act 2001 • Human Rights Act 1998 • Electronic Communications Act 2000 • Computer Misuse Act 1990 • Digital Economy Act 2017

Figure 1: Legal Framework For Digital Forensics (Goldstraw-White, 2022)

In designing policy, procedure and guidance for practitioners, there are extensive codes of practice, manuals, handbooks, standards and guidelines to support

understanding and meet the expectations to provide admissible evidence to the court (Figure 2).

Data Extraction	Data Review	Disclosure	Presentation	Privacy
• ACPO Good Practice Guide for Digital Evidence 2012 • ACPO Good Practice and Advice Guide for Managers of e-Crime Investigations • Criminal Procedure and Investigations Act Code of Practice 2015 • CPS A guide to "reasonable lines of enquiry" and communications evidence 2018 • ENFSI Scenes of Crime Examination Best Practice Manual 2012 • ENISA Basic Guide for first responders 2014 • FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017 • FSS Scenes of Crime Handbook 2004	• Al-Khateeb and Cobley (2015) • ACPO Good Practice Guide for Digital Evidence 2012 • AFSP Standards for the formulation of evaluative forensic science expert opinion 2009 • Common Digital Evidence Storage Format Working Group. (2006) • CPS A guide to "reasonable lines of enquiry" and communications evidence 2018 • ENISA Basic Guide for first responders 2014 • FSR Codes of Practice and Conduct for Forensic Science Providers and Practitioners in the Criminal Justice System 2017 • FSR Guidance: Expert Report Guidance 2019 • Home Office Digital Imaging Procedure 2007	• ACPO Good Practice Guide for Digital Evidence 2012 • Attorney General's Guidelines on disclosure for investigators, prosecutors and defence practitioners 2020 • Criminal Procedure and Investigations Act Code of Practice 2015 • Criminal Procedure Rules and Guide 2015 • CPS Disclosure Manual 2018 • CPS Disclosure - Guidelines on Communications Evidence 2018 • CPS CPS guidance social media offences. 2018 • CPS Guidance for Experts on Disclosure, Unused Material and Case Management 2019	• ACPO Good Practice Guide for Digital Evidence 2012 • AFSP Standards for the formulation of evaluative forensic science expert opinion 2009 • Criminal Procedure Rules and Guide 2015 • Law Commission, Expert Evidence in Criminal Proceedings in England and Wales, 2011 • MoJ Criminal Practice Directions 2015 (and amendments) • Sommer (2017) Digital Evidence Handbook (Kindle edition)	• ACPO Good Practice Guide for Digital Evidence 2012 • Criminal Procedure and Investigations Act Code of Practice 2015 • EC The Privacy and Electronic Communications (EC Directive) Regulations 2003 • HO Interception of communications: code of practice 2016 • House of Commons/House of Lords Joint Committee on Human Rights (2019) (moved from below) • Sommer (2017) Digital Evidence Handbook (Kindle edition)

Figure 2: Policy, Procedure and Guidance Framework for Digital Evidence (Goldstraw-White, 2022).

However, current law regarding extraction, review and disclosure of data is being amended with the introduction of the Police Crime, Sentencing and Courts Act Articles 37 and 38, which aims to provide support for victims in accessing and disclosure of only essential information after the R v Bater and Mohammed case (EWCA, 2020). Previously non-necessary digital communications and evidence were extracted that did not intrude on Article 8 of ECHR.

The Computer Misuse Act 1990 is under review for reform and identifies limitations in the legislation due to technological advancements. There was an 89% increase in computer misuse offences from March 2021 to 2022 (Office for National Statistics, 2022b), and NFIB reported a 4% increase in computer misuse offences from Action Fraud from June 2021 to 2022 (Office for National Statistics, 2022a), which indicates

legislative developments are required, and current legislation is not deterring cybercriminals. Despite the limitations presented, UK law does meet the equivalent EU law due to the Data Protection Act 2018, which defines clear grounds for processing personal data with individuals more control over their data. The legal framework underlines principles of necessity and proportionality to ensure law enforcement whilst safeguarding subjects' rights.

5 Investigative tools

The legal framework relates to all investigations, from identifying, accessing, seizing, and extracting data. Then preserves, stores, transfers, examines, and analyses before submitting evidence in a court of law (Al-Dhaqm et al., 2020). The Forensic Science Regulator (FSR) manages the quality of digital forensic services, which administer codes of practice, and all laboratories must be accredited to ISO/IEC 17025:2017 (ISO, 2018) for competency and impartiality. However, this standard is generic and is not explicitly applied to digital evidence. Digital evidence is governed by the Police and Criminal Evidence Act 1984 (Cyber-Trust, 2018); as such, the National Police Chief's Council (NPCC), in investigations, follow the Association of Chief Police Officers' good practice guide for digital evidence (ACPO, 2012) that underline four critical principles to preserve data, competency record audit trails and manage the process. Whilst this provides a valuable toolkit for practitioners, technology and digital society are rapidly evolving, and the principles should be reviewed for more contemporary approaches (Horsman, 2020).

ISO/IEC 27043:2015 (ISO, 2015) offers an international formal standardised procedure for admissible digital evidence. It is a comprehensive process considering aspects of incident management, secure storage, evidence handling, governance and techniques necessary to produce valid and reliable admissible evidence. The procedures cater for preparation prior to the investigation through the closure and are an idealised international model. Other related standards are used in investigations however are used for different means, such as process-orientated or technology-oriented standards (Valjarević et al., 2016). The process will focus on frameworks and

guidelines whilst technology focuses on exact measures needed, such as how to protect types of storage as ISO/IEC 27040. ISO/IEC 27043:2015 is a process-oriented standard with a high level of detail that spans a wide area of investigative areas and can relate to many other ISO standards, which sets a foundation level for development of other standards, processes or more details procedures.

This investigative framework offers a multifaceted approach rather than a singular strategy. Law enforcement police teams can forge relationships with technological members to maximise resources in a limited time to maximise knowledge and enhance the perception of resilience to cybercrime (Kao, 2017). However, in regional or local law enforcement teams, there are no sufficient standardised procedures to produce quality reports causing inconsistency when investigations are presented. Therefore adhering to standardised methodologies, handling findings by suitably qualified experts and exploring new technologies to ease the standardisation process by employing machine learning without jeopardising the quality of reports (Karie et al., 2019) could be considered.

6 Impact on victims, harm and social perception

Victimology (Turvey, 2014) due to cyber identity theft impacts victims physically and psychologically. Victims endure perceived distress due to the incident, the misuse of personal information, the magnitude of financial loss, and the duration of the investigative process (Li et al., 2019). The case of R v Bater and Mohammed (EWCA, 2020) highlights the impact of collecting necessary personal data so that unnecessary personal information is not made public. The proposed Police, Crime, Sentencing and Courts Act (UK Public General Acts, 2022) defines necessary collection from electronic devices. Physical responses such as headaches and high blood pressure can occur (Reyns and Randa, 2017), with the psychological and emotional distress of depression, anxiety, anger, mistrust and helplessness (Golladay and Holtfreter, 2017) are common responses. The information disclosure in investigations impacts victims significantly, and whilst legislation changes can support future improvements, preventative measures to limit the risk of cyber identity theft could be considered. Examples include password managers against credential breaches, software to prevent malware and education against socially engineered phishing attempts. These measures can be helpful to minimise stress and concern. Fear of the crime of identity theft and victimisation is higher than in other types of crime, which is a factor for perpetrators to target this criminal activity (Choi et al., 2021). However, Gruchola (2022) argues that the media generate fear rather than the direct experience itself (Gruchoła, 2022) due to the internet from mass culture. Fear may play a role in the social perception of cyber identity theft; however, the perception of identity theft as a crime is considered ‘a very serious crime’ by 70% of respondents in the EU (Statista, 2019). Older adults targeted by phishing are considered at risk for cyber identity theft

and cyber fraud due to a reduced sensitivity to the credibility of emails received (Grilli et al., 2020).

7 Conclusion

Cyber identity theft has a significant impact on society. The technological ease and borderless opportunities for criminals to target citizens within the UK have grown on-trend. The adopted changes to current laws on necessary data to be extracted from electronic devices are encouraging to show awareness that all existing legislation should be reviewed to keep up with the technological advancement of society. The current legislation has limitations for recording cyber identity theft as a crime, and the significant amount of law enforcement agencies needed to investigate cases suggests further development of legislation and collaboration regionally, nationally and transnationally. The investigative process has clear codes of conduct to adhere to, which suggests that measures are in place for quality assurance of producing admissible evidence in court, although the judicial outcomes from cases reported are deemed low. Further research should be conducted to identify trends in gender and age for citizens vulnerable to social engineering attempts and opportunities to educate people with preventative measures to reduce criminal activity.

8 References

Acpo. 2012. *ACPO Good Practice Guide for Digital Evidence* [Online]. Available: https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf [Accessed 6 December 2022].

Action Fraud. 2021a. *Cyber Crime Trends* [Online]. Available: https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/CYBER-Dashboard-Assessment-20-21.pdf [Accessed 4 December 2022].

Action Fraud. 2021b. *Reports, referrals and outcomes* [Online]. Available: https://www.actionfraud.police.uk/fraud-stats [Accessed 4 December 2022].

Al-Dhaqm, A., Razak, S. A., Ikuesan, R. A., Kebande, V. R. & Siddique, K. 2020. A Review of Mobile Forensic Investigation Process Models. *IEEE Access,* 8**,** 173359-173375.

Burnap, P., Williams, M., Sloan, L., Rana, O., Housley, W., Edwards, A. & Voss, A. 2014. Tweeting the terror: modelling the social media reaction to the Woolwich terrorist attack. *Social Network Analysis and Mining,* 4**,** 206.

Choi, J., Kruis, N. E. & Choo, K.-S. 2021. Explaining Fear of Identity Theft Victimization Using a Routine Activity Approach. *Journal of Contemporary Criminal Justice,* 37**,** 406-426.

Cifas. 2017. *The Insider Fraud Picture* [Online]. Available: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-2018-09-25-The%20Insider%20Fraud%20Picture%20report-LB-v1_0.pdf [Accessed 4 December 2022].

Cyber-Trust. 2018. *D3.2 Legal analysis of the use of evidence material* [Online]. Available: https://cyber-trust.eu/wp-content/uploads/2020/02/D3.2.pdf [Accessed 6 December 2022].

Edpb. 2021. *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification* [Online]. Available: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf [Accessed 5 December 2022].

Enisa. 2020. *Identity theft* [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-identity-theft [Accessed 10 December 2022].

Ewca. 2020. *R v Carl Bater-James and Sultan Mohammed EWCA Crim 790* [Online]. Available: https://www.bailii.org/ew/cases/EWCA/Crim/2020/790.html [Accessed 6 December 2022].

Ewhc. 2020. *Bilal Hussain Choudhary v Prosecutor at the Creteil Tgi, France* [Online]. Available: https://vlex.co.uk/vid/bilal-hussain-choudhary-v-851096910 [Accessed 5 December 2022].

Fisher, B. & Perkins, C. 2022. *UK Ecommerce Forecast 2022* [Online]. Insider Intelligence. Available: https://www.insiderintelligence.com/content/uk-ecommerce-forecast-2022 [Accessed 4 December 2022].

Goldstraw-White, J. 2022. *Legal and policy framework for digital forensics: A resource for practitioners* [Online]. Available: https://perpetuityresearch.com/wp-content/uploads/2022/09/Final-Legal-Procedural-and-Guidance.pdf [Accessed 6 December 2022].

Golladay, K. & Holtfreter, K. 2017. The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders,* 12**,** 741-760.

Grand Chamber of the European Court of Human Rights. 2021. *Big Brother Watch and Others v. the United Kingdom* [Online]. Available: https://hudoc.echr.coe.int/eng?i=001-210077 [Accessed 5 December 2022].

Grilli, M., Mcveigh, K., Hakim, Z., Wank, A., Getz, S., Levin, B., Ebner, N. & Wilson, R. 2020. Is This Phishing? Older Age Is Associated With Greater Difficulty Discriminating Between Safe and Malicious Emails. *The Journals of Gerontology: Series B,* 76.

Gruchoła, M. 2022. Mass Culture: An Aesthetic Experience or An Experience of Fear? *Studia Gilsoniana,* 11**,** 289-323.

Hasan, I. 2022. *The Data Protection and Digital Information Bill* [Online]. Law Gazette. Available: https://www.lawgazette.co.uk/legal-updates/the-data-protection-and-digital-information-bill/5113758.article [Accessed 5 December 2022].

Horsman, G. 2020. ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports,* 2**,** 100076.

Information Commissioner's Office. 2022. *Case Reference Number INV/0538/2020* [Online]. Available: https://ico.org.uk/media/action-weve-taken/4022280/dfe-reprimand-20221102.pdf [Accessed 5 December 2022].

Intersoft Consulting. N.D. *GDPR* [Online]. Available: https://gdpr-info.eu/ [Accessed 22 January 2022].

Iso. 2015. *ISO/IEC 27043:2015* [Online]. Available: https://www.iso.org/standard/44407.html [Accessed 7 December 2022].

Iso. 2018. *ISO/IEC 17025:2017* [Online]. Available: https://www.iso.org/standard/66912.html#stages [Accessed 6 December 2022].

Kao, D. Y. Exploring the cybercrime investigation framework of ATM Heist from ISO/IEC 27043:2015. 2017 19th International Conference on Advanced Communication Technology (ICACT), 19-22 Feb. 2017 2017. 177-182.

Karie, N. M., Kebande, V. R., Venter, H. S. & Choo, K.-K. R. 2019. On the importance of standardising the process of generating digital forensic reports. *Forensic Science International: Reports,* 1**,** 100008.

Kesteren, J. V., Dijk, J. V. & Mayhew, P. 2014. The International Crime Victims Surveys:A retrospective. *International Review of Victimology,* 20**,** 49-69.

Li, Y., Yazdanmehr, A., Wang, J. & Rao, H. R. 2019. Responding to identity theft: A victimization perspective. *Decision Support Systems,* 121**,** 13-24.

Metropolitan Police. 2022. *More than 100 arrests in UK's biggest ever fraud operation* [Online]. Available: https://news.met.police.uk/news/more-than-100-arrests-in-uks-biggest-ever-fraud-operation-457840 [Accessed 4 December 2022].

Office for National Statistics. 2022a. *Crime in England and Wales: year ending June 2022* [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2022#:~:text=Police%20recorded%20crime%20in%20England,2020%20(6.1%20million%20offences). [Accessed 6 December 2022].

Office for National Statistics. 2022b. *Nature of crime: fraud and computer misuse dataset* [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse [Accessed 6 December 2022].

Official Journal of the European Union. 2021. *European Arrest Warrant and surrender procedures between Member States* [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021IP0006 [Accessed 5 December 2022].

Okeke, R. I. & Eiza, M. H. 2022. The Application of Role-Based Framework in Preventing Internal Identity Theft Related Crimes: A Qualitative Case Study of UK Retail Companies. *Information Systems Frontiers*.

Raab, D. 2022. *Bill of Rights Bill* [Online]. Available: https://bills.parliament.uk/bills/3227 [Accessed 10 December 2022].

Radoini, A. 2020. *Cyber-crime during the COVID-19 Pandemic* [Online]. UNICRI. Available: https://unicri.it/news/cyber-crime-during-covid-19-pandemic#:~:text=According%20to%20the%20report%2C%20in,a%20350%25%20increase%20since%20January.&text=Countries%20all%20across%20the%20globe,in%20cybercrime%20during%20the%20pandemic. [Accessed 4 December 2022].

Reyns, B. W. & Randa, R. 2017. Victim Reporting Behaviors Following Identity Theft Victimization: Results From the National Crime Victimization Survey. *Crime & Delinquency,* 63**,** 814-838.

Statista. 2019. *Perceptions of identity theft as a crime in the European Union (EU) countries in 2018* [Online]. Available:

https://www.statista.com/statistics/1090180/perceptions-of-identity-theft-as-a-crime-eu/ [Accessed 10 December 2022].

Statista. 2022. *How often have you personally experienced online identity theft in the last three years?* [Online]. Available: https://www.statista.com/statistics/480736/frequency-of-experiences-of-online-identity-theft-in-the-united-kingdom-uk/ [Accessed 3 December 2022].

Stevens, A. & Marsons, L. 2022. *Raab's new Bill weakens right remedies* [Online]. The Law Society Gazette. Available: https://edition.pagesuite.com/html5/reader/production/default.aspx?pubname=&edid=6e4deaaf-762b-4411-9ea1-c5c28dc9e9f8&utm_source=gazette_newsletter&utm_medium=email&utm_campaign=Gazette+weekly+edition+9+Dec+2022_12%2f09%2f2022 [Accessed 10 December 2022].

Sumner, S. 2017. *Does GDPR enable identity theft?* [Online]. Computing. Available: https://www.computing.co.uk/news/3021301/does-gdpr-enable-identity-theft [Accessed 5 December 2022].

Turvey, B. E. 2014. Chapter 1 - Victimology: A Brief History with an Introduction to Forensic Victimology. *In:* TURVEY, B. E. (ed.) *Forensic Victimology (Second Edition).* San Diego: Academic Press.

Uk Public General Acts. 2022. *Police, Crime, Sentencing and Courts Act 2022* [Online]. Available:

https://www.legislation.gov.uk/ukpga/2022/32/part/2/chapter/3/enacted [Accessed 10 December 2022].

Valjarević, A., Venter, H. & Petrović, R. ISO/IEC 27043:2015 — Role and application. 2016 24th Telecommunications Forum (TELFOR), 22-23 Nov. 2016 2016. 1-4.

Williams, M. L. 2015. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *The British Journal of Criminology,* 56**,** 21-48.

World Association of Professional Investigators. 2021. *UK: "Identity theft is not a police recordable crime", Action Fraud?* [Online]. Available: https://wapi.org/uk-identity-theft-is-not-a-police-recordable-crime-action-fraud/ [Accessed 6 December 2022].