Exploring Cyber Fraud within the South African Cybersecurity Legal Framework

MM Watney
University of Johannesburg, South Africa

mwatney@uj.ac.za
https://www.orcid.org/0000-0002-1406-7623

Abstract: All countries are globally struggling with the challenges cybercrime presents to the cybersecurity legal framework. Fraud is not a new crime and existed long before the internet. The internet provides a threat actor access to a lot of potential victims and the use of various threat vectors to gain access to personal information by means of social engineering. It is therefore not surprising that cyber fraud has become a serious threat which continues to escalate globally. In 2021, around $100 million was lost in Canada due to online fraud. The United Kingdom (UK) Finance indicated that cyber fraud costs consumers more than £1.2 billion in 2022. The South African (SA) Fraud Prevention Services noted a 356% surge in identity fraud between April 2022 and April 2023. The cybersecurity threat landscape is ever-evolving with the UK Finance warning that the number of cyber frauds could surge out of control as threat actors begin to incorporate the use of Artificial intelligence (AI) to make their operations far more sophisticated and not as easily detected. In 2023 the United States (US) also warned that the irresponsible use of AI could exacerbate societal harms such as fraud. Cyber fraud, also referred to as a "white collar" or commercial crime, is an umbrella term to describe the commission of different types of cyber fraud by means of the use of various threat vectors. The threat vector used to commit the different type of fraud is continuously evolving, such as the use of sophisticated phishing to quishing and deep fakes which are aimed at deceiving the recipient in sharing information. The information obtained from a data breach may be used to commit cyber fraud. Irrespective of the threat vector used to commit fraud, all types of fraud present with the same elements, namely a threat actor who unlawfully and intentionally deceives a victim to benefit and cause harm. The discussion focuses on cyber fraud in general and not a specific type of cyber fraud. The purpose of the discussion is to provide an overview of the challenges cyber fraud present to the South African cybersecurity legal landscape.

Keywords: Cybercrime; Cyber Fraud; South African Cyber Fraud Cybersecurity Legal Framework; Criminalisation of Cyber Fraud; Criminalisation of Conduct Aimed at Obtaining Information; Data Protection and Cyber Fraud

1. Introduction

At the start of 2023, South Africa had 43.48 million internet users and an internet penetration rate of 72%. Social media users stood at 25.80 million people, roughly 42.9% of the total population which stood at 60 million. The number of internet users in the country increased in 2023 by 357,000 (0.8% percent) compared to the same period in 2022 and it continues to grow at a fast rate as South Africa digitalises (Modise, 2023).

As internet penetration and digitalisation grow, so does the risk of becoming a victim of cybercrime increase. A cybercrime can be committed by anyone who has access to a mobile phone and internet connection which makes these crimes relatively easy to commit (Kahle, 2023). It is therefore not surprising that globally the prevention, detection, investigation and prosecution of cybercrime present many challenges. South Africa is ranked 5th in respect of cybercrime victim densities (Kahle, 2023; Labuschagne, 2023). Statics show that cyber fraud is a global concern (Labuschagne, 2023). For example phishing fraud accounted for the most victims, but only led to an average loss of $173 (R3,173) per victim, whereas investment fraud was the most financially-devastating cybercrime in 2022, with total losses estimated to be around $3.3 billion (R60.5 billion), or $108,479 (R2 million) per victim. Tech support fraud is placed second with roughly $807 million (R14.8 billion) in losses, while confidence or romance fraud saw victims losing around $736 million (R13.5 billion). Online payment fraud, credit card fraud, and government impersonation led to losses of $386 million (R7 billion), $264 million (R4.8 billion), and $241 million (R4.4 billion), respectively (Labuschagne, 2023).

Cyber fraud is a non-violent crime characterized by deceit to obtain or avoid losing money, or to gain a personal or business advantage. It is referred to as a "white collar" or commercial crime (Hayes, 2023). The term "white collar" was first coined in 1939 by a sociologist, Edwin Sutherland, who defined it as a crime committed by a person of respectability and high social status (Hayes, 2023).

At the time that the term, "white collar crime", was coined, no one could have foreseen the technological advancements of today and the manner in which it would impact on the commission of fraud. It has moved from a crime committed in a physical medium to one that is predominantly committed online. By moving online, a threat actor have access to more potential victims and many different vectors to access information which was not possible in a physical medium. Threat actors are constantly finding new ways (threat vectors) to deceive or

manipulate or influence users in sharing information, such as phishing fraud. Threat actors are also using generative AI, or deep-learning models which makes it is now easier to produce text, audio and even video, that can deceive, not only potential individual victims, but the security programs used to prevent and detect fraud (Kauflin and Mason; 2023).

Corporations and businesses that fall prey to commercial crime can suffer substantial losses, leading to reputational damage, retrenchments, bankruptcies and economic instability. The erosion of public trust caused by white collar crime stifles economic growth and deters foreign investment.

Internet users need to trust and feel safe and secure online and this can only be achieved by means of robust cybersecurity technical and legal measures. The discussion will show that cyber fraud within the context of South Africa present challenges to the cybersecurity legal framework. The lessons learnt may be also be relevant on a global level as all countries grapple with mitigating cyber fraud.

2. Defining Cyber Fraud as a Form of Cybercrime

Cyber fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another (Hoctor, 2020). All types of fraud consists of deception, for example where an insured person suffered a theft but misrepresents to the insurer the loss suffered by the theft by exaggerating the loss (insurance fraud) or where a threat actor gains unauthorised access to information to assume the identity of the victim (identity theft) and then to commit fraud by opening, for example, accounts in the name of the victim. The aim of the threat actor in general is to profit financially. As indicated, the harm caused by cyber fraud to the victim, whether a natural or legal person, can be devastating.

3. Types of Cyber Fraud and Cyber Vectors

Cyber fraud is a cyber-enabled crime which means that fraud existed prior to the internet, but the Internet is now an instrument by means of which the different types of fraud may be committed. Prior to the internet, it was not easy to gain access to personal information., but the threat vector can use social engineering to deceive users into sharing personal information or to gain access to personal information which in return may be used to commit cyber fraud. At the core of the various cyber fraud is a data breach, and therefore the protection of personal information has become crucial. A Verizon Data Breach Investigation Report found in 2023 that 74% of data breaches have a human element (Stansfield, 2023).

There are different types of fraud that are committed by means of many threat vectors. The threat vectors are all examples of social engineering which is an umbrella term that consists of various tactics aimed at manipulation or deception, such as:

- Identity fraud (Hussain, 2022) occurs when the threat actor gains unauthorised access to a victim's personal information such as full names, identity number, bank account number, and credit card information. The goal of the threat actor may be to use the victim's personal information to commit bank fraud by assuming the victim's identity to access the victim's bank account and stealing the funds or to open and use credit cards in the victim's name and take out loans (credit card fraud) or use the victim's health insurance to pay medical bills(health insurance fraud).
- Phishing is the most common form of cyber fraud with an estimated 3.4 billion spam emails sent every day (Stansfield, 2023; Griffiths, 2024). There are many forms of phishing. It occurs mostly by means of an email, but WhatsApp messages can also be used. The phisher sends emails that appear to be from legitimate sources. They could be emails containing fake invoices, password renewal requests, messages from HR or leadership, and more. The messages often contain links to fake websites designed to access login credentials or other sensitive information. The same email may be sent to many addresses. Phishers can obtain email addresses from places such as corporate websites, existing data breaches, social media platforms, business cards or other publicly available company documents. For example, a user may receive an email from HR prompting them to update passwords by clicking a link. If the email is a phishing email, the link will redirect the user to a website that looks legitimate but has actually been set up by a cyber threat actor. The user then adds their details, which the attacker then uses to gain access to sensitive data and materials. Links to websites may also be infected with malware, such as spyware which can stealthily record sensitive personal and financial information, such as usernames, passwords, and credit card numbers.

Threat actors also try to vish (a combination of the words “voice” and “phishing” conducted by means of a telephone) by obtaining personal information or convincing the victim to install remote access tools that then deploy malicious software to gain entry into the network and data. “Vishers” can use the information and trust developed on these calls to launch effective cyberattacks, such as phishing.

Quishing is also a form of phishing. Quick Response (QR) codes have become an integral part of our daily lives, but with the increasing prevalence comes a new kind of threat, Quishing (a combination of QR code and phishing) is a fraudulent activity where threat actors create malicious QR codes to access sensitive information.

Business Email Compromise (BEC), also sometimes referred to as email fraud, occurs in circumstances in which the threat actor impersonate a known party over email and ask for a change in payment instructions. For example, the threat actor intercepts emails between buyers and sellers by posing as a genuine real estate agent or legal representative. By doing this, they redirect the buyer’s deposit into their accounts (Kahle, 2023). In 2023, the FBI Internet Crime Complaint Center (IC3) released an updated Public Service Announcement, identifying nearly $51 billion in exposed losses due to BEC (Hill, 2023).

In 2020, the South African credit bureau, Experian, was the victim of a BEC in which the threat actor pretended to be a legitimate business. Experian shared business information consisting of various fields including company registration details, general business information, company contact information and credit profile information. Bank account numbers of 24,838 business entities, were shared. The information was shared in May 2020, but Experian only became aware of the fraud in July 2020. Once discovered, Experian notified the affected banks and the Information Regulator in terms of the Protection of Personal Information Act 4 of 2013 (Pieterse, 2020).

- Advance fee fraud occurs when the threat actor deceives a victim into paying for an item or service that never turns up (Tamplin, 2023). An example of advance fee fraud is when a victim is told that they have won a competition or inherited some money from a deceased relative, but need to pay a small fee to release the funds. Once the victim pays the fee, the perpetrator disappears and the promised money is never delivered. In romance fraud the threat actor for example, uses online dating sites and apps to earn his victims' trust, before making up seemingly urgent scenarios to gain his victim's sympathy and steal money from them.
- Ponzi or pyramid schemes may not be preceded by unauthorised access to information, but are based on misrepresenting a fictious investment as an actual investment and thereby misleading the victims. Investment fraud such as Ponzi and pyramid schemes, is a fraudulent scheme that involves paying existing investors in a non-existent enterprise, with funds collected from new investors. A Ponzi scheme promises clients a large profit at little to no risk (Pinkasovitch, 2023). Companies that engage in a Ponzi scheme focus all of their energy into attracting new clients to make investments. This new income is used to pay original investors their returns, marked as a profit from an allegedly legitimate transaction. Ponzi schemes rely on a constant flow of new investments to continue to provide returns to older investors. When this flow runs out, the scheme falls apart.

  A pyramid scheme works a little differently than a Ponzi scheme. This scheme is structured so that the initial schemer must recruit other investors who will continue to recruit other investors, and those investors will then continue to recruit additional investors, and so on (Pinkasovitch, 2023). There comes a time that no new investors can be recruited and the scheme will be exposed.

4. South African Cybersecurity Legislation Governing Cyber Fraud

In the South African context, fraud is defined as the unlawful and intentional making of misrepresentation which causes actual prejudice, or which is potentially prejudicial to another (Hoctor, 2020). Therefore, fraud comprises the following four elements, namely:

- Unlawfulness which refers to conduct that is seen to be wrong in the eyes of society;
- Misrepresentation which refers to a false statement made by one person to another. The misrepresentation may take the form of words; words and conduct; or just conduct or the misrepresentation may also be a failure to disclose certain information in circumstances where there is a duty to do so;

- Intent: The threat actor making the misrepresentation must have intended, or foreseen that the victim would be deceived; and
- Prejudice or potential prejudice: The victim would have suffered prejudice by reason of altering his position to his detriment after relying upon the misrepresentation. Potential prejudice is also sufficient if it is reasonably possible that the victim, relying on the misrepresentation, would have suffered harm.

In 2021 the Cybercrimes Act 19 of 2020 came into operation. It provides for various cybercrimes. Section 8 specifically provides for cyber fraud. As discussed, there are many vectors by means of which a threat actor can gain access to information for the purpose of committing fraud and these threat vectors have been criminalised, such as unauthorised access to information (section 2), interception of data (section 4), the unlawful acquisition, possession receipt and use of passwords, access code or similar data or device to commit fraud. A threat actor can also commit fraud by unlawfully interfering with data or a computer program by deleting data or computer program or alter data or render the data or computer program vulnerable, or damage or deteriorate it (sections 52(a), (b), (c). Fraud can also be committed by interfering with a data storage medium or computer system by altering it (section 6(2)(2)).

The following cybersecurity legislation is relevant as it imposes a report obligation:

1. **The Prevention and Combating of Corrupt Activities Act 12 of 2004 (POCA) requires any offence of** theft, fraud, corruption, forgery, or extortion involving an amount of R100 000 or more to be reported directly to the Directorate of Priority Crime Investigation, more commonly known as the Hawks. The obligation to report these incidents to the Hawks lies on any person in authority, such as the director of a company, manager, CEO, or director-general of a government department) who knows or suspects that any of these offences have been committed. While there is no time limit laid out in the Act for when the report needs to be made, the general rule is that it should be submitted within a reasonable amount of time. Mohamed (2021) opines that if an organisation is going to conduct an investigation into the incident, it would be advisable they wait for the investigation to conclude before reporting the incident in order to present a much more comprehensive report to the authorities.

2. As indicated, a threat actor may unlawfully gain access to data by various means and use the information to commit fraud. The Protection of Personal Information Act 4 of 2003 (POPIA) requires any incidents of a data breach where personal data is reasonably believed to have been compromised, to be reported to the Information Regulator of South Africa, as well as to the subject of that data. POPIA does not have a particular time frame within which the report must be made, but the Act does specifically state that this report must be made as soon as reasonably possible after the discovery of the breach. As such, time is definitely of the essence when it comes to notifying the regulator of a data breach. However, Mohamed (2021) opines that an organisation is able to justify a delay in doing so if the legitimate needs of law enforcement to determine the scope of the breach and restore the integrity of the business' information system, call for it. The Act also notes that an organisation can delay letting the data subject know about the breach if a public body that is responsible for the prevention, detection, or investigation of offences (or the Information Regulator) determines that doing so will impede a criminal investigation. It is important to note that POPIA speaks to the data privacy requirements within South Africa and any business which operates where they must abide by international data laws such as the European Union's General Data Protection Regulation (GDPR) must be cognisant of the requirements thereof. For example, the GDPR requires businesses to report any incident of a data breach not later than 72 hours after having become aware of said breach.

3. In terms of the Financial Intelligence Centre Act (FICA) 38 of 2001 an organisation must report a suspicious and unusual transaction when it becomes aware of it. Under the Act, any person who knows or should know or has suspected that the organisation has received the proceeds of unlawful activities or has facilitated transactions related to the financing of terrorist activities, must report this to the Financial Intelligence Centre (FIC). The same is required when there is knowledge or suspicion of tax evasion or money laundering which must be filed with the FIC under the specific sections of the Act which have been contravened. A report must be made to the FIC within 15 days of the discovery of the incident. Non-compliance is not an option as it could lead to a public reprimand, a remediation directive, the restriction or suspension of certain business activities, and a financial penalty of up to R10 million for a natural person or up to R50 million for a legal person.

4. The reporting obligation in the Cybercrimes Act only applies to electronic communication service providers and financial institutions such as telcos and banks and requires these organisations to report cybercrime

incidents to the South African Police Service within 72 hours of becoming aware of the use of their information systems to commit a cybercrime. The penalty for not doing so in time is R50 000.

Although the specific reporting obligation of an organisation must comply with depends on the specific criminal incident that has occurred, these offences are often interrelated, which may make ignorance of these obligations even more costly for a business or institution. For example, when there is an instance of corruption or fraud, it is usually related to monetary gain and this money may then be laundered in order to avoid raising suspicion. Because of this, an organisation might be beholden to more than one piece of legislation as it relates to reporting one specific incident of commercial crime. Money laundering within the South African context has been challenging as will be shown at paragraph 5 hereafter.

5. Challenges Cyber Fraud Present to the South African Cybersecurity Legal Framework

Threat actors seek to exploit human or security vulnerabilities in order to commit fraud by using different threat vectors. Digital trust in a safe and secure online environment can only be achieved by means of technical and legal cybersecurity measures keeping in mind that the end user presents also a human weakness and risk to the technical measures.

There are many challenges in respect of the legal cybersecurity framework, such as:

1. At the core of many cyber fraud, is unauthorised access to personal information.

   A country must have data protection legislation. It is commendable that South Africa has such legislation, namely POPIA. POPIA imposes a legal duty on the responsible party that processes personal information, to obtain the consent of the user prior to the processing and to have security measures in place to protect the personal information gathered. POPIA is aimed at implementing pro-active security measures to protect personal information. When there is a data breach, then the responsible party has a reporting obligation to the information regulator (discussed at paragraph 4). The time period in which a data breach must be reported, is not outlined in POPIA which in my opinion is a shortcoming.

   In some instances, the victim of fraud, especially identity fraud, only detects it after a long time. Cloete (2023) notes that by the time a victim realises that he is the victim of fraud, the damage has been done as fraudsters may have amassed significant debts in the name of the victim. For example, in the Experian case, referred to at paragraph 4, the credit bureau only realised after approximately 4 months that it had suffered a data fraud and that it had shared a huge amount of personal information with the fraudster. During that period of time, the credit bureau customers were unaware that their information had been shared and could be used to commit fraud.

   Cybersecurity measures are not only aimed at prevention, but must be able to detect the fraud quickly in order for the victim to respond and recover from the harm caused by the deception. However, many of the social engineering are aimed at exploiting human vulnerability to manipulation, and the strongest technical measures can be compromised if the weakest link, end user, do not take precautions. Constant cybersecurity awareness training is crucial to internet users, irrespective of whether they are bank clients or employees.

2. No cybersecurity technical measures are infallible and there may be a security compromise. Kauflin and Mason (2023) also opine that generative AI "could ultimately make obsolete, state-of-the-art fraud-prevention measures such as voice authentication and even "liveness checks" designed to match a real-time image with the one on record".

   A country must have comprehensive cybercrime legislation. Cybercrime legislation is re-active, in other words, the investigation takes place only once the case has been reported. If there is a delay in reporting the cyber fraud to the police, then the evidence needed to prove the commission of the fraud could potentially be lost, deleted or destroyed.

   South Africa has the Cybercrimes Act which provides for cyber-dependant and cyber-enabled crimes. There are many threat vectors by means of which the threat actor can gain access to information which is used to commit fraud and these vectors have been criminalised.

   In 2023 it was reported that an estimated 90% of cybercrimes go unreported in South Africa (Kahle, 2023). Crime reporting serves an important purpose; namely preventing a threat actor from continuing with this type of criminal behaviour which protects the public in general from becoming a victim of cyber fraud.

There are various reasons why only 10% of cybercrime cases are reported to the police:

- The victim may not trust that the police will be able to effectively investigate the case or may not have confidence in the criminal justice system that the case will go on trial.

  The police who are tasked with the investigation of a cybercrime, such as identifying the threat actor (perpetrator) and gathering of the evidence, may not have the relevant investigative skills or assistance to effectively investigate a matter, especially in circumstances where the security compromise is committed outside of South Africa. In this regard, South Africa is not unique as the nature of cybercrime challenges law enforcement globally. Unlike a physical crime, the threat actor does not have to be physically close to the victim to commit a crime and technology allows the crime to occur outside the country's borders in which instance the police need assistance from the other country's law enforcement.

- A victim may wish not to report the cyber fraud out of fear that the disclosure will affect its' reputation negatively. There are legislation that imposes a compulsory reporting obligation. Compliance with such legislation must be enforced.

3. Preventing the use of the proceeds of cybercrime, such as those obtained from fraud by means of money laundering, has proven a challenge. A country must ensure enforcement and compliance with anti-money laundering legislation. For purposes of this discussion, it should be noted that in 2023 South Africa was greylisted by the global financial crime watchdog, the Financial Action Task Force (FATF) for not fully complying with international standards around the prevention of money laundering, terrorist financing and proliferation financing. As indicated, threat actors target the human aspect of security. For example, "money muling" instances increased by 97% in 2021 (Cloete, 2023). "Money muling" occurs when a money mule transfers or moves illegally acquired money on behalf of someone else and in return the mule receives monetary compensation (Cloete, 2023).

4. BEC and liability for the BEC continue to be a serious concern for companies of all industries and sizes. Courts have had to deliberate whether a business could be held civilly liable for the economic loss suffered by a client as a result of a BEC. The court determined that a business that makes use of emails for payments, must forewarn their clients of the potential risk of fraud and take the necessary security precautions to safeguard against the risk of harm from a possible BEC. If a business does not forewarn a client nor take reasonable security steps to safeguard against a BEC, the business may be held liable for the financial loss suffered by the client who became a victim of cyber fraud as a result of negligence on the side of the business (Orekeng, 2023).

6. Conclusion

A robust technical and legal cybersecurity framework can go a long way in preventing cyber fraud.

Unfortunately, the weakest link in cybersecurity is the human vulnerability to social engineering. The human end user may be deceived, manipulated or influenced by means of various vectors to share information which in turn may be used to commit a cybercrime, such as cyber fraud. Over the years, the threat actor has become more sophisticated in the use of the threat vector which at times can be very convincing, especially now with the use of AI. The role of cybersecurity awareness training in combatting social engineering cannot be over-emphasised. Likewise the role of financial education in safeguarding investors against Ponzi and pyramid schemes cannot be downplayed. These "investments" exploit human vulnerability to manipulation. Propositions promising exceptional returns at minimal risk should be treated with a high degree of scepticism as these offers are frequently indicative of fraudulent schemes.

Even if the human aspect of technical cybersecurity is addressed, technical measures may be compromised, especially as AI may be used by the threat actor to compromise the technical security measures. In the case of a security compromise, the cyber fraud must be reported to the police to ensure an investigation and possible prosecution of the crime. By means of strong legislation, prescribed reporting obligations within specific timelines, effective enforcement, mutual cross-border assistance, and stringent punishment, a threat actor will realise that "white collar" crimes will not be tolerated. It will also restore trust in the criminal justice system. A zero tolerance approach to cyber fraud will contribute to digital trust. Digital trust enables individuals and businesses to engage online with the confidence that their information is secure against cyber threats, such as cyber fraud.

References

Beard, J. (2023) “Fraudsters need just 3 seconds on a cold call to clone your voice…and scam your family”, https://www.thisismoney.co.uk/money/beatthescammers/article-12615607/Fraudsters-need-just-3-seconds-cold-call-clone-voice-scam-family.html.

Cloete, N. (2023) “Experts concerned as cybercrime cost South Africans billion”; [online]; https://www.iol.co.za/saturday-star/news/experts-concerned-as-cybercrimes-cost-south-africa-billions-0b0fc4ce-0b1f-410c-a953-8985fb1543a1.

Griffiths, C. (2024) “The latest 2023 phishing statistics (updated January 2024)”; [online]; https://aag-it.com/the-latest-phishing-statistics/.

Hayes, A. (2023) “What is white collar crime? Meaning, types and differences” [online]; https://www.investopedia.com/terms/w/white-collar-crime.asp.

Hoctor, S. (2020) Snyman’s Criminal Law; LexisNexis (Pty) Ltd; pages 461 – 409.

Kahle, C. (2023) “Going beyond ‘Nigerian Prince’: SA turning into Africa’s cybercrime capital”, [online], https://www.citizen.co.za/lifestyle/technology/south-africa-turning-into-cybercrime-capital/.

Kauflin, J. and Mason, E. (2023) “How AI is supercharging financial fraud – and making it harder to spot”; [online]; https://www.forbesafrica.com/daily-cover-story/2023/09/19/how-ai-is-supercharging-financial-fraud-and-making-it-harder-to-spot/.

Labuschagne, H. (2023) “South Africa n world’s top 5 worse countries for cybercrime”; ;[online]; https://mybroadband.co.za/news/security/489183-south-africa-in-worlds-top-5-worst-countries-for-cybercrime.html.

Lawton, G. (2023) “How to prevent deepfakes in the era of generative AI”, [online],https://www.techtarget.com/searchsecurity/tip/How-to-prevent-deepfakes-in-the-era-of-generative-AI.

Modise, E. (2023) “28% of South Africans have no internet connectivity”; [online]; https://techcabal.com/2023/04/06/internet-connectivity-south-africa-2023/.

Mohamed, Z. (2021); “4 Commercial crime reporting obligations organisations must comply with”; online; https://www.lexology.com/library/detail.aspx?g=a7c59e90-b24c-421f-a96b-e5e33c106256.

Orekeng, K. (2023) “The dangers of business email compromise” De Rebus; [online]; https://www.derebus.org.za/the-dangers-of-business-e-mail-compromise/.

Pinkasovitch, (2023) A. ”Ponsi scheme vs Pyramid scheme: What is the difference?”: [online], https://www.investopedia.com/ask/answers/09/ponzi-vs-pyramid.asp.

Stansfield, S. (2023) “Verizon Data Breach Investigations Report 2023: Our Top Takeaways”, [online], https://www.vadesecure.com/en/blog/verizon-data-breach-report-2023.

Tamplin, T. (2023) “Advance Fee Fraud”; [online]; https://www.financestrategists.com/wealth-management/investments/advance-fee-fraud/.