Concerns About the Social Layer of Cyberspace: Analyses of Recent Cybercrime Cases and the Prospect of IFA's Developing Role

Research Project for Emerging Issues/Advanced Topics Course

Master of Forensic Accounting Program, University of Toronto

Prepared by Mina Holie

June 13, 2023

For Prof. Leonard Brooks

Abstract

As we see increasing cybercrimes and fraud, the growth of cyber vulnerabilities is relentless in the IT-enabled environment. Through the analyses of actual cybercrime cases, the objectives of this research are to examine, as the landscape of cybercrime has evolved, how the approaches to fraud prevention, detection, and investigation have evolved as well as to delve into what major commonalities and obstacles are. Subsequently, in consideration of the emerging issues, the implications for the investigative and forensic accounting (IFA) education and professional practice will be explored. This paper is intended for a general body of the IFA; hence, the technicalities of cybersecurity are less focused. Key finding: In cybercrime, the social engineering techniques are often employed—as human factors can increase the chance of certain events from occurring, productively. Recommendation: The IFA practitioners should equip themselves with up-to-date knowledge and collaborate with experts in different disciplines to deepen their understanding of unique circumstances pertinent to cyberspace. Conclusion: Consider the vulnerable factors from human, technological, legal, socioeconomic, and geographical perspectives and keep your skepticism and investigative mindset towards cyberspace.

Keywords: cybercrime, cyberspace, IT, cybersecurity, cyberattack, fraud, bribery, corruption, social engineering, money laundering, cryptocurrency, information system, risk, IFA, forensic, investigation

Table of Contents

Motive of the Research

To effectively achieve business goals and objectives, various sectors have been upgrading their core business functions and business operating systems to take advantage of new digital tools and digitized work processes. Hence, information technology (IT) and digitized information have impacted on our daily life and every organization in forming the digital environment worldwide. Under the influence of such an evolving situation, cybercrimes have been increasing significantly because of our reliance on the IT-enabled services.[1] Accordingly, many organizations have seen significant demands for implementing, maintaining, and protecting their critical IT infrastructure as having real-time situational awareness and assessment.[2] As a result of lack of the proper IT environment management and the security awareness training, organizations could face negative consequences such as disruption or interruption of day-to-day operations, inaccessibility to or loss of data, financial loss, damage to reputation, etc. Furthermore, the recent COVID-19 pandemic significantly changed the landscape of cyber threats and cybercrimes as our daily habits and lifestyle changed, including the way of work.[3] Indeed, Canadian organizations have experienced losses due to cybercrimes and fraud at

1. Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2016," December 6, 2021. https://doi.org/10.2813/275589
2. Ursillo, Steve, Jr., and Christopher Arnold, "Cybersecurity Is Critical for all Organizations – Large and Small," *International Federation of Accountants*, November 4, 2019. Accessed on May 15, 2023, from https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small
3. Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," October 28, 2022. Accessed on May 14, 2023, from https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

a historic high in 2022.[4] In addition to taking this crisis as an opportunity, cybercriminals and fraudsters took advantage of such existing issues with the IT infrastructure's susceptibility to cyber risk; COVID-19 rather enhanced and consequently complicated one of the existing vulnerabilities—the human as a drawback.[5]

Problem Statement and Objectives

The cyber breach and information theft incidents are not purely IT problems.[6] Moreover, the significant factor of such incidents would inextricably be linked to traditional techniques—social engineering.[7] According to European Union Agency for Cybersecurity (ENISA), social engineering techniques have always existed, as a way of drawing out personal or confidential information by the use of manipulation and deception, but evolved in combination with digital tools, platforms, and their pertinent processes; this shift has resulted in various types of cybercrimes.[8]

An endpoint can be any device that is physically connected to a network, such as servers, desktop computers, laptops, mobile phones, virtual machines, and the Internet of things (IoT) including various types of sensors, routers, security systems, wearable

4. Royal Canadian Mounted Police, News Release, "Fraud Prevention Month 2023: Fraud losses in Canada reach another historic level," February 27, 2023. https://www.rcmp-grc.gc.ca/en/news/2023/fraud-prevention-month-2023-fraud-losses-canada-reach-historic-level
5. European Union Agency for Network and Information Security, "Cyber Security Culture in organisations," November 2017. https://doi.org/10.2824/10543; Swanson, Scott, "The role of fraud examinations in cybercrime," *Fraud Magazine*, August 2015. https://www.fraud-magazine.com/article.aspx?id=4294989368
6. Ibid., 5.
7. Ibid., 1.
8. European Union Agency for Cybersecurity, "What is 'Social Engineering'?," 2023. Accessed on May 20, 2023, from https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

technology, etc.[9] These devices are called the cyber threat surface because threat actors target such Internet-exposed endpoints, as gateways to valuable assets, which are dependent on human behaviour.[10] What is more, human factors have played a key role not only in perpetrating cybercrimes but also in intercepting such offenses.[11] Hence, this evolving situation would be affecting the role and investigative techniques of investigative and forensic accounting (IFA) practitioners. As the digital environment has enabled threat actors to emerge from anywhere in the world, this has become a global concern.[12] Due to this evolving situation, a question would arise: How should the IFA practitioners equip themselves to tackle this type of crime?

Thus, the objectives of this research are to examine, as the landscape of cybercrime has evolved, how the approaches to fraud prevention, detection, and investigation have evolved as well as to delve into what major commonalities and obstacles are through the analyses of the following cybercrime cases: Sanjay Madan, FTX Trading Ltd., and Amazon.com, Inc. Subsequently, in consideration of the emerging issues, while the technicalities of cybersecurity would be less focused, the implications and hence recommended approaches to the IFA education and professional practice will be explored.

---

9. Microsoft, "What is an endpoint?," *Microsoft Security*, 2023. Accessed on May 20, 2023, from https://www.microsoft.com/en-ca/security/business/security-101/what-is-an-endpoint
10. Canadian Centre for Cyber Security, "An introduction to the cyber threat environment," October 28, 2022. Accessed on May 14, 2023, from https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment
11. Ibid., 5.
12. House of Commons, Evidence, "Standing Committee on Industry, Science and Technology," May 20, 2020, Number 016, 43rd Parliament, 1st Session. https://www.ourcommons.ca/Content/Committee/431/INDU/Evidence/EV10761671/INDUEV16-E.PDF

Background Information: Two Types of Cybercrimes

Cybercrime, its nature is often complex. Although there is no formal definition, it is generally said that cybercrimes are offenses related to computer devices, computer networks, and/or digital data and that offenders and victims are often located in geographically different areas.[13] This type of offenses would be divided into three categories: offenses specific to the Internet (cyberattacks such as malware, phishing, and ransomware), cyberfraud and online forgery (user manipulation and data alteration for deprivation of property or money, including identity thefts), and illicit digital content (online abuse and exploitation for extortion, coercion, and incitement to or glorification of violence, terrorism, hatred, etc.).[14] Contrary to traditional fraud cases, cybercrimes are difficult to deal with because of the lack of paper audit trails, the need of knowledge of technology used to commit an offense or affected by it, or the involvement of experts from various domains.[15] In addition, depending on how the technology is employed for what purpose, these offenses can also be categorized further into cyber-dependent crime and cyber-enabled crime.[16]

13. United Nations Office on Drugs and Crime (UNODC), "Global Programme on Cybercrime," n.d. Accessed on May 21, 2023, from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
14. European Commission (EC), "Cybercrime," *Directorate-General for Migration and Home Affairs*, n.d. Accessed on May 21, 2023, from https://home-affairs.ec.europa.eu/cybercrime_en
15. Association of Certified Fraud Examiners (ACFE), "Cyberfraud," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 1, 1.1401.
16. Crown Prosecution Service, Legal Guidance, "Cybercrime - prosecution guidance," September 26, 2019. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Cyber-Dependent Crime

Cyber-dependent crime is an offense that can be committed only by the use of technology.[17] In other words, it needs the IT infrastructure to execute it; therefore, its vulnerability could put it at risk. Interconnected by communication links, data communication networks transmit various types of data such as text, images, voice, videos, digital files, etc. The components of their transmission systems require to process, transmit, and send/receive data, going through a set of communication protocols.[18] In this case, a device can be used as a tool to commit an offense or become a target of the offense to be committed. Some of such examples are as follows:

- Intrusion into digital assets such as devices, networks, and data
- Disruption or interruption of services or functionality through malware or ransomware[19]

These offenses may be committed by highly skilled individuals or groups but with low criminal intent such as hacktivists, while they may be committed by organized criminals, cyberterrorists, or employees who have the capacity to do so (e.g., privileged access to IT systems as well as adequate knowledge and skills to use IT tools).[20]

Technicalities of Systems Interconnection in IT Infrastructure

Originally developed by the International Organization for Standardization (ISO), the Open Systems Interconnection (OSI) model is a conceptual framework presented with seven different layers according to the logical model of networking or telecommunication

17. Ibid., 16.
18. IBM, "The Fundamentals of Networking," n.d. Accessed on May 14, 2023, from https://www.ibm.com/topics/networking
19. Ibid., 16.
20. Ibid., 16.

systems; therefore, this framework makes it useful in the cybersecurity field as it can help diagnose possible vulnerabilities and incoming attacks.[21] The OSI model's each layer from the bottom to the top is as follows:

- Layer 1: Physical layer representing the electrical and physical representation of the systems such as networking devices, antennas, cables, etc.
- Layer 2: Data link layer acting as a connecting link between two nodes in the network and breaking up packets into frames, which contain protocols necessary to route data
- Layer 3: Network layer organizing to route data between networks through the best available path
- Layer 4: Transport layer facilitating the transmission of data sequence, tracking data packets, and providing flow and error controls
- Layer 5: Session layer creating communication channels to coordinate sessions between servers and managing activities as a checkpoint of data transfers such as the authentication and authorization of communication
- Layer 6: Presentation layer converting data formats between the application and network as formatting, encrypting, compressing, decrypting, and again formatting data to prepare data for the application layer

21. International Organization for Standardization, "ISO/IEC 7498-1:1994(en) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model – Part 1," November 15, 1994. https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-1:ed-1:v2:en; Turay, Brima, "Analysis of Seven Layered Architecture of OSI Model," *Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS)*, December 13, 2019, Vol. 2, Iss. 12, 73-77. https://ssrn.com/abstract=3815237; "What are the 7 layers of the OSI model?," *DataDome*, October 24, 2021. Accessed on May 14, 2023, from https://datadome.co/learning-center/7-layers-osi-model/

- Layer 7: Application layer sending and receiving meaningful data to directly interact with end users for various services at the application level[22]

In Layer 1 to Layer 6, most of known vulnerabilities are due to either physical or technical issues such as lack of proper physical access control or network security protocols inadequately configured in the systems; therefore, they can be prevented or mitigated through physical or technical control measures.[23] On the other hand, Layer 7 is the most vulnerable and so needs the strong IT governance and security control since end-user interactions are the most significant at the application level and the most complex to manage, directly sending and receiving data—this layer is not easy to prevent or mitigate cyberattacks only by strengthening networks and systems because human factors are highly involved.[24]

Inevitable Link with Cyber-Enabled Crime

For the segment humans significantly interact such as the application layer, their decision, action, and influence are always key factors for interference, manipulation, and intervention in the IT infrastructure, which are often conducted in a coordinated manner.[25] Although this type of cybercrime is committed only by the use of technology, some techniques and purposes found among cyber-dependent crime are employed in combination with attacks on the most vulnerable characteristics of Layer 7—human interactions. Because of this reason, the cyber-enabled crime side cannot be slighted.

22. Ibid., 21.
23. Ibid., 21.
24. Ibid., 21.
25. Smith, Jonathan, "Biotech Startups Face a Growing Wave of Cyberattacks," *Labiotech*, June 25, 2022. Accessed on May 14, 2023, from https://www.labiotech.eu/in-depth/cyberattack-biotech-startups-covid/

Cyber-Enabled Crime

Cyber-enabled crime is an offense that is like traditional crime with no use of technology but has extended in scale or transformed in reach through the technology.[26] Some of such examples are as follows:

- Economic crime such as fraud, forgery, sabotage, corruption, data theft, and money laundering
- Online marketplaces for unfair competition and illegal items such as counterfeits and pirated goods
- Malicious communication such as extorting, coercing, bullying, and trolling, which would include psychological manipulation techniques like social engineering to exploit human error[27]

Because the technology has allowed it to transition to a different level, there are different scope and approaches to committing this type of offense, in comparison with its traditional forms.[28]

Major Characteristics

The most apparent characteristics of cyber-enabled crime are the use of psychological manipulation techniques against humans—social engineering.[29] Some instances of such recent cybercrime cases are of Sanjay Madan, FTX Trading Ltd., and Amazon.com, Inc. Accordingly, these cases are closely examined in the subsequent sections.

26. Ibid., 16.
27. Ibid., 16.
28. Ibid., 16.
29. Europol, "The Internet Organised Crime Threat Assessment (IOCTA) 2018," January 11, 2019. https://doi.org/10.2813/858843

Analyses of Cybercrime Cases

In essence, cybercrimes are committed because of various elements and their vulnerable factors, such as human, technological, legal, socioeconomic, and geographical elements. Hence, the following four cybercrime cases were selected to closely examine in taking into these elements into account:

1. Sanjay Madan case (Canada)
2. FTX case (global)
3. Amazon cases (global)
    - Internal corruption
    - Ephraim (Ed) Rosenberg

Human and Technological Elements: Sanjay Madan

Case Facts

In light of the COVID-19 pandemic, the governments around the world were taking action in an effort to provide financial support to their citizens. The Government of Ontario was one of them, offering relief funds through the Support for Families Program (SFFP). Sanjay Madan (also known as Sadanand Madan) was formerly an IT director of the Ontario Ministry of Education ("Ontario") and has admitted committing two fraud schemes: misappropriation of funds from the SFFP and kickbacks through Ontario's recruitment of IT fee-for-service consultants.[30] As Ontario's senior IT

30. Arsenych, Alex, "Former government employee pleads guilty to stealing $47.4-million from Ontario," *CTV News Toronto*, April 4, 2023. Accessed on May 18, 2023, from https://toronto.ctvnews.ca/former-government-employee-pleads-guilty-to-stealing-47-4-million-from-ontario-1.6342662; Her Majesty the Queen in Right of Ontario v. Madan et al., 2022 ONSC 1538 (CanLII). https://canlii.ca/t/jn5xk; Her Majesty the Queen in Right of Ontario v. Madan, 2022 ONSC 5103 (CanLII). https://canlii.ca/t/jrt19

personnel, Madan helped develop an application for the SFFP and had access to its payment processing system, while his family members have denied any involvement and rather accused the Crown of failing to properly supervise the government employee and put controls in place for the prevention of fraud.[31]

For the SFFP funds misappropriation, he has been alleged to have stolen $11 million, which was equivalent to the total amount paid to about 43,000 to 54,000 children, by making false applications with false identities and having the funds deposited into Madan's bank accounts.[32] After one of his banks contacted Madan about suspicious transactions, he took action to try to conceal possible evidence of fraud by deleting a database he falsified and wiping his computer.[33]

In addition, it was discovered during the SFFP fraud allegations that he was receiving illegal payments, in total of about $30 million, intended as compensation from the IT consulting vendors of his choice for at least 10 years.[34] Because of these fraudulent activities, the Crown obtained a Mareva injunction to freeze the Madan

31. Perkel, Colin, The Canadian Press, "'I felt betrayed': Family denies helping father who allegedly stole $11M in Ontario COVID relief," *National Post*, January 26, 2021. Accessed on May 18, 2023, from https://nationalpost.com/news/canada/civil-servant-betrayed-family-with-alleged-11-million-covid-relief-fraud-docs; His Majesty the King in Right of Ontario v. Madan, 2022 ONSC 5355 (CanLII). https://canlii.ca/t/js0pv
32. Ibid., 30.
33. Lou, Ethan, "Easy Money: The scam that revealed chaos and a culture of fraud at Queen's Park," *Toronto Life*, May 25, 2021. Accessed on May 20, 2023, from https://torontolife.com/city/the-scam-that-revealed-chaos-and-a-culture-of-fraud-at-queens-park/; Star Editorial Board, "The security lapse that cost Ontario taxpayers," *Toronto Star*, April 14, 2023. Accessed on May 20, 2023, from https://www.thestar.com/opinion/editorials/2023/04/14/the-security-lapse-that-cost-ontario-taxpayers.html
34. Ibid., 30.

family's worldwide assets.[35] While Madan has been sentenced to 10 years in prison, this case is still ongoing at the pleadings stage at the time of this paper being written.[36]

Analysis of the Case

Although Madan was known as being thrifty at his workplace, he had a very comfortable lifestyle in possession of multiple luxurious properties, a pleasure craft, and rental apartment buildings of 30 units.[37] This is typical of the characteristics of fraudsters.[38]

The issue of kickbacks is a traditional type of procurement fraud—having a conflict of interest and undue influence on dealing with particular vendors in the award bidding process for the purpose of receiving compensation. In other words, this would be of an ethical issue and bribery of the public official, which allowed him to employ ghost vendors for IT consulting.[39] Apart from Madan's other fraudulent act, this could have been detected and prevented by having the monitoring process and procurement procedures that are proportionate with legal and business compliance requirements as well as the segregation of duties.[40]

35. HMQ v. Madan, 2020 ONSC 8093 (CanLII). https://canlii.ca/t/jcr9t
36. D'Mello, Colin, "Former Ontario government employee pleads guilty to multi-million dollar fraud," *Global News,* April 4, 2023. Accessed on May 18, 2023, from https://globalnews.ca/news/9601082/former-ontario-government-employee-guilty-plea-multi-million-dollar-fraud/; His Majesty the King in Right of Ontario v. Madan, 2023 ONSC 2831 (CanLII). https://canlii.ca/t/jx6tg
37. Ibid., 33.
38. ACFE, "Corruption," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 1, 1.625.
39. Ibid., 36.
40. Organisation for Economic Co-operation and Development (OECD), United Nations Office on Drugs and Crime (UNODC), World Bank, "Anti-Corruption Ethics and Compliance Handbook for Business," 2013. https://www.oecd.org/corruption/anti-corruptionethicscompliancehandbook.pdf

On the other hand, the other fraudulent case of the SFFP is an example of employee fraud with the use of Ontario's information systems, which is considered cyber-enabled crime. Madan opened thousands of bank accounts under his own name and his family members' names at multiple financial institutions with the intention of having the relief funds deposited into those accounts, which he has admitted under oath.[41] He used the IT knowledge, skillset, and job position as his advantage to launder taxpayers' money. He had the capability to exercise a lucrative incentive and opportunities for the malicious, selfish purpose because a large sum of money was just made accessible in light of the unusual pandemic, in rationalizing that all of his activities would not be detected.[42]

Indeed, at the development stage of the SFFP application, it was possible for Madan to plan for this fraudulent scheme in creating or finding security holes and internal control gaps; he knew that Ontario maintains only a list of school children in the public school system, not those in private school or home-schooled.[43] Then, as creating the fake database of the SFFP applicants with thousands of names and addresses by web scraping software, he was able to develop and use the opportunities through the SFFP's information systems to manipulate its application process and payment processing portal.[44] Furthermore, he managed to maneuver his subordinate into removing a system security alert by deceit and keep the security protocols loosen despite the proper security protocols in place within the ministry; the COVID-19 situation also helped make his

41. Ibid., 30.
42. Ibid., 33.
43. Ibid., 33.
44. Ibid., 30.

staff's mind wandered as no precedent.[45] Moreover, in addition to hiring a student in India for false application submissions, he used his another subordinate with false information, which was told highly confidential, to bypass the Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA).[46] Because of his senior position in the ministry, he had little oversight but significant authority for decision-making; therefore, he was able to maneuver people around him and abuse the information systems.[47]

Technological and Legal Elements: FTX Trading Ltd.

Case Facts

Known as FTX, this company used to operate the cryptocurrency exchange and crypto hedge fund, buying/selling cryptos and gathering money from investors to invest in digital asset projects. In 2019, Sam Bankman-Fried and Gary Wang founded FTX in Nassau, The Bahamas; it was one of the largest crypto exchanges in the world, which was worth $32 billion as of January 2022, until its bankruptcy was declared in November 2022.[48] Due to FTX's collapse, numerous investors from well-known companies to individual investors were significantly affected; some of the notable ones are Google,

45. Ibid., 33.
46. Ibid., 33.
47. Ibid., 33.
48. "FTX - Crunchbase Investor Profile & Investments," *Crunchbase*, 2023. Accessed on May 20, 2023, from https://www.crunchbase.com/organization/ftx-exchange; Elder, Bryce, and Alexandra Scaggs, "The FTX bankruptcy filing in full (updated)," *Financial Times*, November 17, 2022. Accessed on May 20, 2023, from https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d; Hetler, Amanda, "FTX scam explained: Everything you need to know," *TechTarget*, April 17, 2023. Accessed on May 20, 2023, from https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know

Meta, Netflix, TikTok, Twitter, Apple, Amazon, Microsoft, and celebrities like Tom Brady and Kevin O'Leary who were advocating FTX.[49] Even the company like Chainalysis, a US blockchain analysis firm that does virtual currency investigations for government agencies, became a victim of FTX's collapse, having previously worked for two joint forces to update the crypto industry's anti-money laundering (AML) and know-your-customer (KYC) frameworks.[50]

While taking deposits from customers and trading cryptocurrencies including its own digital token FTT on its platform, FTX was unable to meet the demand for their withdrawals—the traditional banking problem as a bank run.[51] It first appeared to be that way, due to an accounting oversight; however, it was rather due to fraud in coordination with Alameda Research ("Alameda"), which was also founded by Bankman-Fried, and in collusion with Wang and Nishad Singh, chief engineer, of FTX, who manipulated the codes written in the FTX platform so that Alameda could unlimitedly keep borrowing

49. Emerson, Sarah, "FTX Owes Money To Every Major Tech Company, Including Google, Meta, Amazon And Apple," *Forbes*, January 26, 2023. Accessed on May 20, 2023, from https://www.forbes.com/sites/sarahemerson/2023/01/26/ftx-owes-money-to-every-major-tech-company-google-meta-amazon-tiktok-apple/; Silverman, Sam, "From Tom Brady to Kevin O'Leary - See Who Lost Big in the Wake of the FTX Crypto Collapse," *Entrepreneur*, January 25, 2023. Accessed on May 20, 2023, from https://www.entrepreneur.com/business-news/who-lost-money-in-ftx-tom-brady-kevin-oleary-and-more/443653
50. Brown, Kimberly, Docket # 574, "List of Creditors (Verification of Creditors Matrix) Filed by FTX Trading Ltd.," Case 22-11068-JTD, Chapter 11, District of Delaware, United States Bankruptcy Court, January 25, 2023. https://document.epiq11.com/document/getdocumentbycode?docId=4142165&projectCode=FTX&source=DM; Key, Alys, "Chainalysis Confirmed as FTX Creditor in Bankruptcy Case," *Decrypt*, November 17, 2022. Accessed on May 22, 2023, from https://decrypt.co/114931/chainalysis-confirmed-ftx-creditor-bankruptcy-case
51. Andrieu, Thomas, "Crypto And FTX: The Return Of The Bank Run In The 21st Century," *GoldBroker*, November 15, 2022. Accessed on May 20, 2023, from https://goldbroker.com/news/cryptos-ftx-return-bank-run-21st-century-2915

money from FTX's customer deposits.[52] This closely tied sister company heavily relied on FTX's customer funds for borrowing, while the balance sheet was not prepared to show its assets and liabilities; this mishandling was uncovered when the acquisition deal offered from Binance fell through—this was the time when the massive withdrawal and decrease of FTT's value happened.[53] Consequently, Bankman-Fried decided to remove an option to withdraw money on FTX's platform so that the customers cannot access their funds because there was the gap of about $8 billion between the amounts owed and able to pay—this lack of liquidity led to the bankruptcy.[54] Once this news became known to the public, similar activities such as mass withdrawals and account suspension were observed among other cryptocurrency companies around the world at an alarming rate; FTX's malpractice and collapse caused contagion in the digital currency exchange (DCE) industry worldwide.[55]

52. Ibid., 48; Berwick, A., Shiffman, J., and K. Gui Qing, "Exclusive: How a secret software change allowed FTX to use client money," *Reuters*, December 13, 2022. Accessed on June 8, 2023, from https://www.reuters.com/technology/how-secret-software-change-allowed-ftx-use-client-money-2022-12-13/; Securities and Exchange Commission, Plaintiff, v. Nishad Singh, Defendant, Case 1:23-cv-01691, Southern District of New York, United States District Court, February 28, 2023, para. 5. https://www.sec.gov/litigation/complaints/2023/comp25652.pdf
53. Ibid., 48.
54. Ibid., 48.
55. Associated Press, "The downfall of FTX's Sam Bankman-Fried sends shockwaves through the crypto world," *NPR*, November 14, 2022. Accessed on May 22, 2023, from https://www.npr.org/2022/11/14/1136482889/ftx-sam-bankman-fried-shockwaves-crypto

In January 2023, the U.S. Securities and Exchange Commission (SEC) charged Bankman-Fried with defrauding the investors and concealing the diversion of their funds for his own investment and personal purposes.[56] In May 2023, Bankman-Fried's lawyers filed motions to dismiss the multiple fraud charges against him, and this case is still ongoing with more hearings to be held.[57]

Analysis of the Case

The regulations for cryptocurrency are still developing and evolving, and so is the cryptocurrency itself. FTX deposits were not insured by the Federal Deposit Insurance Corporation (FDIC) of the United States. Originally, in August 2022, the FDIC issued a cease-and-desist letter for FTX's misrepresentation about its deposits made by the customers, in following FTX's misleading Twitter post implying that the deposits would be covered by insurance; the FDIC regarded this tweeting done by the then CEO Brett Harrison as a warning sign of the misrepresentation given to the public.[58]

56. U.S. Securities and Exchange Commission (SEC), Litigation Release No. 25616, "Securities and Exchange Commission v. Samuel Bankman-Fried, No. 1:22-cv-10501 (S.D.N.Y. filed Dec. 13, 2022)," January 19, 2023. https://www.sec.gov/litigation/litreleases/2023/lr25616.htm
57. Scannell, Kara, and Allison Morrow, "Sam Bankman-Fried wants his case thrown out of court," *CNN Business*, May 8, 2023. Accessed on May 22, 2023, from https://www.cnn.com/2023/05/08/tech/sbf-ftx-dismissal-hnk-intl/index.html; Epiq Systems, Inc., "FTX Trading Official Committee of Unsecured Creditors," Case # 22-11068, November 11, 2022. Accessed on May 23, 2023, from https://dm.epiq11.com/case/ftx/info
58. Federal Deposit Insurance Corporation (FDIC), Press Releases, "Potential Violations of Section 18(a)(4) of the Federal Deposit insurance Act," August 18, 2022. https://www.fdic.gov/news/press-releases/2022/ftx-harrison-letter.pdf

In North America including The Bahamas, the deposit insurance does not apply to virtual assets held in a non-bank financial institution like FTX.[59] Since there are also concerns about the implications of cryptocurrency trading for money laundering, the Digital Asset Anti-Money Laundering Act was introduced by the United States Senate in December 2022 for the AML purposes.[60] Yet, there are no legal protections for deposited crypto funds and their value, which could significantly fluctuate rapidly without warning.

The application of existing regulatory frameworks to the virtual assets is still unfamiliar and challenging to many organizations around the world; the global standards for regulating crypto assets are still underway.[61] In Africa, Asia, and Oceania, the crypto laws and regulations are yet inconsistent, unsettled, and/or significantly or partly pending,

59. FDIC, Fact Sheet, "What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies," July 28, 2022. https://www.fdic.gov/news/fact-sheets/crypto-fact-sheet-7-28-22.pdf; Deposit Insurance Corporation (DIC) Bahamas, "Who are DIC Member Institutions?," December 23, 2022. Accessed on May 22, 2023, from https://www.dic.bs/di-members.php; Office of the Superintendent of Financial Institutions (OSFI), Statement, "Statement to entities engaging in crypto-asset activities or crypto-related services," November 16, 2022. https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/Pages/20221116_let.aspx
60. Warren, Elizabeth, Press Releases, "Warren, Marshall Introduce Bipartisan Legislation to Crack Down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations," *U.S. Senator Elizabeth Warren of Massachusetts*, December 14, 2022. https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations
61. Narain, Aditya, and Marina Moretti, Publications, "Regulating Crypto," *International Monetary Fund (IMF)*, September 2022. https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti

in taking the risk of financial market volatility into consideration.[62] On the other hand, the countries like Japan and Switzerland have established crypto laws and regulations for the user protections and AML purposes.[63] In addition, in the European Union (EU), Markets in Crypto-Assets (MiCA), a new crypto regulation in EU law, was approved in April 2023 and will come into force in 2024 as the world's first comprehensive regulatory framework.[64] Yet, for the majority of the world, they are still at the regulatory consultation and drafting stages.[65]

62. Fuje, H., Quayyum, S., and T. Molosiwa, Blog, "Africa's Growing Crypto Market Needs Better Regulations," *IMF*, November 22, 2022. Accessed on May 23, 2023, from https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations; "Cryptocurrency regulation diverges across Asia," *Economist Intelligence Unit (EIU)*, February 8, 2022. Accessed on May 23, 2023, from https://www.eiu.com/n/cryptocurrency-regulation-diverges-across-asia/
63. Arora, Gaurav, "Cryptoasset Regulatory Framework in Japan," *Social Science Research Network (SSRN)*, November 19, 2020. https://doi.org/10.2139/ssrn.3720230; Financial Services Agency (FSA) 金融庁, Policy, "Summary of the Systematization of Legal Infrastructure Related to Crypto Assets 暗号資産（仮想通貨）に関連する制度整備について," April 7, 2021. https://www.fsa.go.jp/policy/virtual_currency/20210407_seidogaiyou.pdf; Regulated United Europe (RUE), "Crypto Regulations in Switzerland," 2023. Accessed on May 23, 2023, from https://rue.ee/crypto-regulations/switzerland/; State Secretariat for International Finance (SIF), "Blockchain / DLT," December 23, 2022. Accessed on May 23, 2023, from https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html
64. European Parliament, Press Releases, "Crypto-assets: green light to new rules for tracing transfers in the EU," April 20, 2023. https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu; Council of the European Union, Press Release, "Digital finance: Council adopts new rules on markets in crypto-assets (MiCA)," May 16, 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/
65. Securities Commission of the Bahamas, Media Release, "IOSCO Sets the Standard for Global Crypto Regulation," *International Organization of Securities Commissions (IOSCO)*, May 23, 2023. https://www.scb.gov.bs/wp-content/uploads/2023/05/IOSCONEWS693.pdf

As mentioned above, the legal infrastructure as to crypto assets has been evolving as urged to be established effectively and globally in a coordinated manner, especially in light of this FTX case, to protect users from fraudsters and opportunists and avert criminal activities such as misappropriation, money laundering, and crypto-cleansing for terrorist financing, drug/human trafficking, etc. in the virtual assets market where all of these are, after all, codes in cyberspace.

One of such fraudsters and opportunists was Bankman-Fried, taking the situation at that time as the opportunity as seeing legal gaps, ambiguity, and complexity as to crypto assets. Indeed, he was trying to even influence political parties as to how the cryptocurrency should be regulated by giving them large donations.[66] He used the FTX customers' virtual funds to fund bets on his investment for Alameda Research, despite a violation of the securities law, and to maintain his comfortable lifestyle and have possession of multiple luxurious properties.[67]

It was not just a cyber version of the Ponzi scheme, in which the success depends on the ability to bring in more investors as existing investors are paid by the money obtained from new investors.[68] In the FTX case, there is the gap of about $8 billion.[69] Although the virtual assets cannot be wiped out completely from cyberspace, they can

66. Ibid., 56; Kolhatkar, Sheelah, "How Serious Are Sam Bankman-Fried's Alleged Campaign-Finance Violations?," *The New Yorker*, January 11, 2023. Accessed on May 24, 2023, from https://www.newyorker.com/business/currency/how-serious-are-sam-bankman-frieds-alleged-campaign-finance-violations
67. Ibid., 56.
68. SEC, "Ponzi Scheme," *Investor.gov*, n.d. Accessed on May 24, 2023, from https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme
69. Ibid., 48.

still be lost.[70] Further, it is possible for those with the IT knowledge to create one's own cryptocurrency token by utilizing a pre-built, open-source blockchain platform like Ethereum, which already comes with the smart contract functionality (protocol to automatically test and determine if predetermined conditions are met or agreements are in line for the program execution); the FTT token was a centralized exchange on the FTX platform where customers had little control over their funds.[71] This fact might have been part of driving forces behind Bankman-Fried's motivation to divert the funds into different purposes as customers cannot see such transactions through their computer monitors. This yet poorly regulated market was where he could rationalize or slight a series of his actions.

Socioeconomic and Geographical Elements: Amazon.com, Inc.

Headquartered in the United States as one of the largest technology companies in the world, Amazon is a global company that operates e-commerce, cloud computing, and digital services such as subscriptions (membership, digital entertainment, e-books, etc.) and advertising.[72] Amazon's revenues from its international segment generally consist of e-commerce (both buyers and sellers), subscriptions, and AWS; about 66 to 72 % of the total net sales was generated from the e-commerce operations of online stores and

70. Gomzin, Slava, *Crypto Basics: A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors*, 1e, Berkeley, CA: Apress, 2022. https://doi.org/10.1007/978-1-4842-8321-9; "What is Ethereum?," *ethereum.org*, 2023. Accessed on June 1, 2023, from https://ethereum.org/en/what-is-ethereum/; "FTX (FTT): Its Downfall & The Launch of FTX 2.0," *Bybit Learn*, May 29, 2023. Accessed on June 1, 2023, from https://learn.bybit.com/crypto/what-is-ftt/
71. Ibid., 70.
72. Amazon.com, Inc., *2022 Amazon Annual Report*, February 2, 2023. https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_AMZN_2022.pdf

third-party seller services in the past three years, according to Amazon's 2022 annual report.[73] Therefore, the e-commerce is a primary source of earnings for this company.

Its e-commerce platform Amazon Marketplace was launched in November 2000; at that time, Amazon was the one-of-a-kind online retailer where customers, as consumers or small business owners, could buy and/or sell products on the same website.[74] While this company's business is still evolving at the present time, this two-sided, cross-border marketplace business model transformed the retail industry and significantly influenced today's consumer behaviour and shopping habits globally.[75]

Case Facts #1 – Internal Corruption

The U.S. Department of Justice (DOJ) charged six individuals with bribery and fraud schemes that were committed in Amazon Marketplace; one of them was a former

73. Ibid., 72.
74. Allen, Lizzie, Press Center, "Amazon Marketplace a Winner for Customers, Sellers and Industry; New Service Grows over 200 Percent in First Four Months," *Amazon*, March 18, 2001. Accessed on May 27, 2023, from https://press.aboutamazon.com/2001/3/amazon-marketplace-a-winner-for-customers-sellers-and-industry-new-service-grows-over-200-percent-in-first-four-months
75. Mello-Klein, Cody, "Amazon is transforming what a small business is–and it looks just like Amazon. Is that a good thing?," *Northeastern Global News*, January 27, 2023. Accessed on May 27, 2023, from https://news.northeastern.edu/2023/01/27/amazon-small-business-transformation/

Amazon employee Rohit Kadimisetty, sentenced to imprisonment in the United States.[76] As having previously worked as a seller support employee out of India, Kadimisetty bribed Amazon employees and contractors in India, after having moved to the United States, to interfere with fair competition in the marketplace on a global scale.[77] Forming a conspiracy to commit bribery with other individuals, he gained control over the marketplace platform to pass on third-party sellers' search and ranking algorithms and the other confidential information to their competitors.[78] Furthermore, prompted through bribes, counterfeit or unsafe goods were sold by bypassing the Amazon Marketplace rules to restore some accounts under suspension and using artificial intelligence (AI) algorithms to promote such goods; on the other hand, the competitors' listings were ruined by posting fake negative reviews or suspending the sale of products as their orchestrated attacks.[79] By abusing the insiders' privileged access to information systems and third-party sellers' data, he manipulated the marketplace platform to create

76. Palmer, Annie, "DOJ charges six people in scheme to bribe Amazon employees to 'gain upper hand' on marketplace," *CNBC*, September 18, 2020. Accessed on May 27, 2023, from https://www.cnbc.com/2020/09/18/doj-charges-six-people-in-scheme-to-bribe-amazon-employees.html; Palmer, Annie, "Former Amazon employee sentenced to 10 months in prison for involvement in bribery scheme," *CNBC*, February 11, 2022. Accessed on May 27, 2023, from https://www.cnbc.com/2022/02/11/former-amazon-employee-sentenced-to-10-months-in-bribery-scheme.html; United States Attorney's Office, Western District of Washington, Press Release, "First of six consultants indicted in Amazon bribery scheme sentenced to prison," *U.S. Department of Justice (DOJ)*, February 11, 2022. https://www.justice.gov/usao-wdwa/pr/first-six-consultants-indicted-amazon-bribery-scheme-sentenced-prison
77. Ibid., 76.
78. Ibid., 76.
79. Ibid., 76.

advantageous conditions for certain sellers and, as a result, had them garner over $100 million in competitive benefits.[80]

Case Facts #2 – Ephraim (Ed) Rosenberg

Ed Rosenberg has been a well-known Amazon consultant for third-party sellers and a founder of the consulting company Amazon Sellers Group TG (ASGTG), stating on the ASGTG website that he is a compliance specialist.[81] On March 27, 2023, he posted the following comment on his YouTube channel:

> For a time, some years ago, I began to obtain and use Amazon's internal annotations—Amazon's private property—to learn the reasons for sellers' suspensions, in order to assist them in getting reinstated…I paid bribes, directly and indirectly, to Amazon employees…I should not have engaged in any of this conduct. I am sorry to have done these things. I very much regret doing them. I will be pleading guilty in federal court to a crime for this misconduct. I promise that I will not do this again.[82]

Rosenberg pleaded guilty to bribing Amazon employees in exchange for the confidential, insider information to support the third-party sellers in solving their issues with Amazon and educate them about how to boost their sales in Amazon Marketplace—he was not

80. Ibid., 76.
81. "How Amazon Seller's Group Began," *Amazon Sellers Group TG (ASGTG)*, n.d. Accessed on June 3, 2023, from https://www.asgtg.com/about/; Palmer, Annie, "Amazon seller consultant admits to bribing employees to help clients; will plead guilty," *CNBC*, March 27, 2023. Accessed on June 3, 2023, from https://www.cnbc.com/2023/03/27/amazon-seller-consultant-admits-to-bribing-employees-to-help-clients.html
82. Rosenberg, Ed, [Amazon Sellers Group TG], *Apology From Ed Rosenberg.* [Video], YouTube, March 27, 2023, paras. 2-3. Accessed on June 3, 2023, from https://www.youtube.com/watch?v=v410zJ46Mpk

only creating unfair advantage but also committing a crime, rather than legitimately navigating them to become successful small business owners as a compliance/suspension consultant.[83] Prior to posting his statement above on the day he admitted his wrongdoing in court, he was claiming that he was just framed up for the allegations; however, he suddenly changed his plea and acknowledged that his conduct was corrupt and unacceptable.[84] While this case is still ongoing as considered significantly complex by court, his latest trial was scheduled on May 15, 2023; no court document has been made accessible to the public yet this year.[85]

Analyses of the Two Cases

Both cases are interconnected with the bribery schemes committed in exchange of inducing a favourable situation for their own benefit—control over the marketplace by capitalizing on the corrupt insiders' capacity, such as privileged access to information systems and internal data as employees, and their ability to abuse internal control weaknesses such as lack of technical and administrative oversight of accessing and handling the proprietary data. Kadimisetty exploited his insider knowledge and contacts obtained through his previous workplace as well as money as his tools, seeing as an advantageous opportunity, to orchestrate the schemes; this might have served as an incentive for his conduct. Further, to conceal his identity, he was using misleading email

83. Ibid., 81.
84. Ibid., 81; Ibid., 82.
85. Steiner, Ina, "Well Known Amazon Consultant to Plead in Bribery Case," *EcommerceBytes*, March 25, 2023. Accessed on June 3, 2023, from https://www.ecommercebytes.com/2023/03/25/well-known-amazon-consultant-to-plead-in-bribery-case/; United States of America, Plaintiff, v. Ephraim Rosenberg and Hadis Nuhanovic, Defendant, Case 2:20-cr-00151-RAJ, Western District of Washington, United States District Court, July 18, 2022. https://casetext.com/case/united-states-v-rosenberg-51

accounts and encrypted messages when communicating with the insiders; he might have been rationalizing that all of his activities would not be caught.[86]

Moreover, in Rosenberg's case, he plotted this bribery scheme not only to get himself paid for subscriptions (monthly retainers) and regular consulting (some services offered free of charge to attract clients) but also to gain his professional reputation as a consultant who can effectively solve his clients' issues with "Ed's extensive knowledge of Amazon and proven high success rate."[87] In fact, he has been praised as an incredible consultant within the ASGTG community and has still been operating his company to date despite his corrupt conduct, holding networking events and discussion meetings to actively interact with Amazon third-party sellers online and in person.[88] Therefore, the purposes of maintaining his reputation and competence in problem-solving and gaining more clients might have served as incentives as he has seen an opportunity for consulting because of many troubled Amazon third-party sellers, in rationalizing that he is helping those small business owners achieve their goals. Having admitted his wrongdoing, he now candidly says that "I strongly encourage all sellers and seller consultants to follow my lead on this."[89] It seems that, regardless of whatever ways, he wants to stay in a position to lead.

86. Ibid., 76.
87. "Contact Ed," *ASGTG*, n.d. Accessed on June 3, 2023, from https://www.asgtg.com/contact/
88. "ASGTG 2023," *ASGTG*, 2023. Accessed on June 3, 2023, from https://www.asgtg.com/event/asgtg-2023/; Rosenberg, Ed, [Amazon Sellers Group TG], *EU Kyc Funds Held FBA Blocked Company Address Verification Issue. Great Info For Amazon* [Video], YouTube, May 22, 2023. Accessed on June 3, 2023, from https://www.youtube.com/watch?v=AxTg7GBUy6k
89. Ibid., 82.

Comparative Review of the Four Cases

Similarities

Power. The most significant point among all four cases is the fact that Madan (Ontario), Bankman-Fried (FTX), Kadimisetty (Amazon), and Rosenberg (Amazon) were playing God as if they would have held power over other people and organizations for the consequences of a series of events encompassing them.

Madan. He was in the senior IT position within the ministry, having little oversight and yet significant authority; he could tell his subordinates what to do even for something against regular protocols—capacity. In addition, the pandemic situation also helped utilize a unique circumstance and trick his staff's mind with deceit while he had access to the information systems as having helped develop the SFFP program including its application—opportunities. He could exploit the critical gaps such as Ontario's internal control weaknesses (inadequate information security measures, the incomplete list of children as fund recipients, management override of internal controls, etc.) when Ontario made a large sum of money accessible in light of the pandemic—incentives. He had already been successful in defrauding taxpayers' money for about 10 years through another scheme; he thought he could get away with this second scheme again—rationalization. Madan was enjoying his comfortable lifestyle in possession of luxurious properties, while keeping control of the systems, data, and people's inclination.

Bankman-Fried. He is a founder of FTX, having had no oversight and yet ultimate authority; in collusion with the other individuals, he embedded the codes in the crypto platform so that Alameda could keep extracting FTX's customer deposits—capacity. In addition, the public's view about cryptocurrency's ambiguity and complex

issues also helped him play around and get away with loopholes while the governments around the world had still been drafting or discussing new crypto laws and regulations—opportunities. He exploited such critical gaps in the preexisting legal framework and the defenseless crypto platform intentionally built, which FTX's customers would never know about, and they just kept pouring a large sum of money into a black hole in cyberspace in the hope of getting a high rate of return—incentives. He did not expect to be knocked out by the bank run in such an old-fashioned way in the high-tech environment; he might have thought that he could get away with moving the customer funds around without public knowledge, although he still insists that he did not try to commit fraud on anybody, having merely acknowledged his conduct as mistake—rationalization.[90] Bankman-Fried was enjoying his comfortable lifestyle in possession of luxurious properties, while keeping control of the systems, stream of ciphers, and people's optimism.

Kadimisetty. He was a former employee of Amazon, having had his internal knowledge and contacts gained within the company during his employment; he knew whom to contact at the Indian office location to successfully carry out his schemes remotely—capacity. In addition, the two-sided, cross-border marketplace business model, where third-party sellers compete with each other to attract attention from potential buyers all around the world, helped him exploit such favourable circumstances for him while he could have knowledge of how to optimize search and ranking results through certain algorithms and boost the number of shoppers' visits—opportunities. He

90. Evans, Pete, "'I didn't ever try to commit fraud on anyone,' FTX founder Sam Bankman-Fried says," *CBC News*, November 30, 2022. Accessed on June 5, 2023, from https://www.cbc.ca/news/business/ftx-sam-bankman-fried-1.6669767

knew that there were a large number of suspended accounts of which the sellers were desperate to sell off counterfeits and/or unsafe goods—incentives. He was creating unfair advantage in the marketplace by manipulating Amazon employees in India, cyberbullying against certain sellers' competitors, and masterminding all through his computer monitor from out of country; he thought he could get away with this scheme just by masking his online identity and using encrypted messaging services—rationalization. Kadimisetty was taking advantage of socioeconomic inequality out of the United States, while keeping control of the systems, environmental imbalance (e.g., the nature of Amazon Marketplace, socioeconomic, geographical, etc.) and people's greed.

Rosenberg. He has been a well-known consultant and a founder of ASGTG, being admired within the ASGTG community in the world and relied on as a leader among online small business owners; he has had direct contacts with Amazon employees because of his consulting work in solving the compliance issues—capacity. In addition, he sees that such sellers have been facing difficulty in maintaining their Amazon Business accounts to sell their merchandise for whatever reason, being asked for help as a compliance/suspension specialist—opportunities. He wanted to boost his fame and promote his reputation even more as an ultimate problem solver and educator to obtain more clients; therefore, he had to continue to be successful in smoothing out their issues and giving them effective advice to improve their business, calling himself the Amazon knowledge expert—incentives. He was believing that, although obtaining confidential, internal information from Amazon employees in such an improper way that had resulted in ruining fair competition, he was still helping those troubled small business owners and that they were really appreciating his help—rationalization. Rosenberg was taking

advantage of his professional status, while keeping control of the influence on systems, environmental imbalance (e.g., the nature of Amazon Marketplace, socioeconomic, privilege, etc.), and people's attachment.

Existence of All Factors in the Fraud Diamond. In the above four cases, there are all four conditions of the fraud diamond met, which is an extension of the fraud triangle theory (opportunities, incentives, and rationalization plus the capacity factor).[91] Madan, Bankman-Fried, and Rosenberg were in the position of superior and/or authority while Kadimisetty exploited his prior knowledge and contacts obtained during his employment; regardless, all of them had knowledge, skills, and/or abilities necessary to commit crime. Madan and Bankman-Fried were both in the environment where they could orchestrate the schemes from the very early stage to create or identify vulnerabilities within the systems and utilize them for their benefits, while Kadimisetty and Rosenberg found opportunities because of how Amazon Marketplace operates. Both Madan and Bankman-Fried saw a large sum of money in front of them, while both Kadimisetty and Rosenberg saw a large number of third-party sellers having difficulty in maintaining their business accounts for merchandise sale. Madan, Bankman-Fried, and Kadimisetty did not expect that they would get caught that way, while Rosenberg thought he was yet making a contribution to problem-solving and boosting their business

91. Verma, Raina, "How Fraudsters Exploit the Capabilities of Contract Employees to Conduct Their Schemes," *ACFE Insights*, July 28, 2021. Accessed on June 4, 2023, from https://www.acfeinsights.com/acfe-insights/how-fraudsters-exploit-the-capabilities-of-contract-employees-to-conduct-their-schemes; ACFE, "Data Analysis and Reporting Tools," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 2, 3.701-3.749.

(although he was taking some sellers' opportunities away through creating unfair advantage); regardless, all of them were rationalizing their conduct.

All Incidents Happened in Layer 7 of the OSI Model. The schemes in all four cases were carried out in the most vulnerable application layer, where human interactions are the most significant and hence the most difficult to manage even when security protocols and internal controls are properly in place. Since humans directly deal with endpoint devices to transmit data for a variety of reasons and intent, this layer has to be protected from cyber risk in a mixed approach, in combination with technical, administrative, and physical security controls.[92] As regarded as the cyber-enabled crimes, Madan, Bankman-Fried, Kadimisetty, and Rosenberg used the social engineering techniques as their means of drawing out the confidential information from others or exploiting the vulnerable systems and processes in combination with digital tools, digital platforms, and bribes.[93]

Never Acted Alone. Madan, Bankman-Fried, Kadimisetty, and Rosenberg did not act alone in order to successfully execute their schemes. Madan had the collaborators outside of the Ontario government as well as overseas; in addition, using his senior position and deceit, he was also using his subordinates who had no knowledge of what he was committing. While yet insisting on his no knowledge of how to code, Bankman-Fried could have built the ill-considered crypto trading platform with his

92. Ibid., 21; Ibid., 29; Albeda, Jouke, "Are IT General Controls Outdated? Data Protection and Internal Control Over Financial Reporting," *Information Systems Audit and Control Association (ISACA) Journal*, December 28, 2022, Vol. 6. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/are-it-general-controls-outdated
93. Ibid., 8.

co-founder and working partners in collusion.[94] Kadimisetty coordinated his schemes with Amazon employees who were then working at the office location he used to work. Rosenberg also obtained the proprietary data from Amazon employees, manipulating their judgment and behaviour by bribes.

Differences

By contraries, there were some differences found among the four cases in considering different aspects.

Geographical Scale. Madan's schemes were committed within Canada, although money was laundered overseas, and his collaborators had resided overseas as well. The schemes committed by Bankman-Fried, Kadimisetty, and Rosenberg significantly impacted on investors, buyers, and sellers all around the world because both FTX and Amazon are global companies.

Transparency of the Identity and Action. While Madan's subordinates saw his unusual activities at workplace, the others were manipulating the systems, information, and people remotely. Furthermore, while Kadimisetty was masking his identity for impersonation by the misleading email accounts and encryption, no investors could know or see Bankman-Fried's action. On the other hand, Rosenberg was dealing with the stakeholders as himself, Amazon compliance/suspension consultant.

94. Ibid., 52; Irwin, Kate, "Sam Bankman-Fried Says FTX Hacker May Be a Former Employee," *Decrypt*, November 29, 2022. Accessed on June 5, 2023, from https://decrypt.co/115963/sam-bankman-fried-ftx-hacker-former-employee; Bhole, Aneeta, "Sam Bankman-Fried's 'secret' $65 BILLION backdoor: FTX boss ordered co-founder to insert a single number into millions of lines of code to funnel clients' cash, attorneys claim," *Daily Mail*, January 14, 2023. Accessed on June 5, 2023, from https://www.dailymail.co.uk/news/article-11635721/Sam-Bankman-Fried-ordered-FTX-founder-create-secret-backdoor-Alameda-Research.html

Attitude Throughout the Course of Schemes. While Madan was overriding the existing security controls, exploiting internal control weaknesses, creating the fictitious database, and manually bypassing the CAPTCHA, Bankman-Fried was in conspiracy to embed the malicious codes within FTX's crypto trading platform at the inception stage of the company; they were both active from the beginning. On the other hand, for both Amazon cases, their conduct was derived from the work experience, as either an Amazon employee or an Amazon consultant, with Amazon customers and employees; they turned into an active role after observing the situations in a passive environment.

Gaps in Legal/Regulatory Frameworks or Organizational Policies/Protocols. Bankman-Fried could play around the ambiguity, complexity, and incompleteness of crypto laws and regulations. On the other hand, in Ontario and Amazon, there were organizational policies and protocols in place; however, they were breached or overridden. In other words, such administrative security controls did not work effectively as intended, which means that more layers of security controls would have been required.

Excess Appetite for Money and/or Fame. It appears that Madan, Bankman-Fried, and Kadimisetty committed crime because of money. Furthermore, for Madan and Bankman-Fried, they could see a large sum of money through their computer monitors sitting in the accounts, which were both manipulable by them. On the other hand, for Rosenberg, although it is likely, he might have been just eager to solve the third-party sellers' issues and pass on his knowledge to his followers—this could also result in obtaining more future clients and hence more revenues with more reputation.

Major Risk Factors

"There is no patch for human stupidity," it is said in the phycology field.[95] The above four cases identified human, technological, legal, socioeconomic, and geographical vulnerabilities that allowed cyber-enabled crimes to happen. For all of these vulnerabilities, the social engineering techniques were employed—as human factors can increase the chance of certain events (unfavourable for most but beneficial for cybercriminals and fraudsters) from occurring, productively. The application layer of the OSI model is the most susceptible to human vulnerability because every human has partiality for something or someone; at the same time, low cognitive effort can cause biased judgment.[96] Thus, to manipulate people to have them do things that might not be in their best interests, the tricks on human behaviour, social practice, and mental processes are blended in for decision-making.[97] Then, the evolution of communication added further complexity to this issue because of the technological development.[98]

95. Anonymous, as cited in Hadnagy, Christopher, "A Deep Dive Into Human Vulnerability," *Psychology Today*, May 15, 2022, para. 2. Accessed on June 5, 2023, from https://www.psychologytoday.com/ca/blog/human-hacking/202205/deep-dive-human-vulnerability
96. Ibid., 21; Goel, S., Williams, K., and E. Dincelli, "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems (JAIS)*, January 31, 2017, Vol. 18, Iss. 1, 22-44. https://doi.org/10.17705/1jais.00447; Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., and G. Russello, "SoK: Human-centered Phishing Susceptibility," *Association for Computing Machinery (ACM) Journal*, April 14, 2023, Vol. 26, Iss. 3, Article 24, 1-27. https://doi.org/10.1145/3575797
97. Hadnagy, Christopher, "A Deep Dive Into Human Vulnerability," *Psychology Today*, May 15, 2022. Accessed on June 5, 2023, from https://www.psychologytoday.com/ca/blog/human-hacking/202205/deep-dive-human-vulnerability
98. Wang, Z., Sun, L., and H. Zhu, "Defining Social Engineering in Cybersecurity," *Institute of Electrical and Electronics Engineers (IEEE) Access*, May 19, 2020, Vol. 8, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

Prevention Perspectives

People and Processes

For the Madan case, Ontario's internal controls were inadequate to mitigate IT security risks—excessive confidence in employees' goodwill. Although security policies and protocols were in place, adequate oversight was lacking due to his senior position. The segregation of duty and the project inspection at the executive level could prevent Madan from successfully executing his schemes. For the FTX case, it must have been difficult to prevent its scheme, unless there were regulatory requirements of external auditing, since the founders and their working partners created a backdoor within the crypto platform at the inception of the company so that the customer deposits would flow into Alameda without the customers' consent.[99] For the Amazon cases, there were also internal controls in place; furthermore, this company has had a cybersecurity team of 12,000 employees working globally to fight against fraud in collaboration with local law enforcement agencies.[100] However, they were not able to prevent the international bribery schemes or the creation of unfair advantage committed by the former and then current employees.

99. Ibid., 94.
100. Berthiaume, Dan, "Exclusive: Amazon exec discusses how company is fighting online fraud," *Chain Store Age (CSA)*, December 1, 2022. Accessed on June 6, 2023, from https://chainstoreage.com/exclusive-amazon-exec-discusses-how-company-fighting-online-fraud

Laws and Regulations

Antitrust. The violation of antitrust laws was a huge deal for Amazon—significant impact on its reputation and finances globally. Although Amazon has lost its appeal against the European Commission (EC)'s move, as to double antitrust probes, to the European Court of Justice (ECJ) this year, this company had still managed to settle with the EC, without paying a fine, by making several commitments agreed upon, such as not using non-public data of third-party sellers and their activities through Amazon's automated tools or employees.[101] Yet, if the commitments are breached in the next seven years, Amazon will have to pay a fine up to 10% of the total annual turnover.[102] These EC's three-year antitrust probes ended; however, Amazon has also held multiple antitrust issues in the other continents.

101. Chee, Foo Yun, "Amazon may face EU antitrust charges over merchant data in coming weeks: source," *Reuters*, June 11, 2020. Accessed on June 8, 2023, from https://www.reuters.com/article/us-eu-amazon-com-antitrust-idCAKBN23I2V7; Chee, Foo Yun, "Amazon settlement with EU antitrust regulators possible by year end -sources," *Reuters*, November 25, 2022. Accessed on June 8, 2023, from https://www.reuters.com/technology/amazon-settlement-with-eu-antitrust-regulators-possible-by-year-end-sources-2022-11-25/; EC, Press Release, "Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime," December 20, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777; Bodoni, Stephanie, "Amazon Loses EU Court Fight Over Double Antitrust Sales Probes," *BNN Bloomberg*, April 20, 2023. Accessed on June 8, 2023, from https://www.bnnbloomberg.ca/amazon-loses-eu-court-fight-over-double-antitrust-sales-probes-1.1910031
102. Ibid., 101.

In Japan, Amazon had been investigated by the Japan Fair Trade Commission (JFTC) for different issues—the company itself was unreasonably asking third-party sellers to pay part of the costs of discount, calling it a collaboration fee, by abusing its position superior to the sellers.[103] Amazon settled with the JFTC upon the agreement about demands that the collaboration fees be returned to those third-party sellers, in total of about $18.8 million.[104] In North America, the antitrust lawsuits by the Federal Trade Commission (FTC) of the United Sates are getting underway, and the Canadian antitrust case will rather go to arbitration.[105] Amazon's antitrust issues derived both internally and externally and caused contagion globally; as a result, the trade commissions have established news rules and demanded to fulfill Amazon's commitments as preventive and corrective measures.[106]

103. Gibbs, Samuel, "Amazon's Japanese headquarters raided by nation's regulator," *The Guardian*, March 15, 2018. Accessed on June 8, 2023, from https://www.theguardian.com/technology/2018/mar/15/amazon-japanese-headquarters-raided-regulator-antitrust-fair-trade-commission; "Amazon Japan returns $18m to suppliers in deal with Tokyo," *Nikkei Asia*, September 11, 2020. Accessed on June 8, 2023, from https://asia.nikkei.com/Business/Companies/Amazon-Japan-returns-18m-to-suppliers-in-deal-with-Tokyo; Japan Fair Trade Commission (JFTC), Press Releases, "Approval of the Commitment Plan submitted by Amazon Japan G.K.," September 10, 2020. https://www.jftc.go.jp/en/pressreleases/yearly-2020/September/200910.html
104. Ibid., 103.
105. Sisco, Josh, "Washington prepares for war with Amazon," *Politico*, March 20, 2023. Accessed on June 8, 2023, from https://www.politico.com/news/2023/03/20/ftc-amazon-irobot-antitrust-00087711; "Canadian Federal Court Rules Amazon Price-Fixing Case Will Go to Arbitration," *Competition Policy International (CPI)*, October 13, 2022. Accessed on June 8, 2023, from https://www.competitionpolicyinternational.com/canadian-federal-court-rules-amazon-price-fixing-case-will-go-to-arbitration/
106. Ibid., 101; Ibid., 103; Ibid., 105.

Cryptocurrency. In light of the FTC case, the governments around the world have been urged to establish crypto laws and regulations, while Japan, Switzerland, and the EU have been going ahead of the others in terms of regulating cryptocurrency. Such regulatory frameworks might serve as preventive measures due to possible close scrutiny and regulatory requirements.

Detection Perspectives

Cognitive Biases

People can miss a warning sign in every possible situation because of cognitive biases; we may have cognitive errors that can lead to wrong thoughts, decisions, and executions.[107] For the Madan case, his subordinates had been given some unusual tasks such as asking to keep the information system security protocols loosen, by removing the security alert, and bypass the CAPTCHA manually despite the existing protocols. They knew Madan's such requests were not in accordance with such protocols. However, Canadians had heard the prime minister's briefing on the pandemic saying that, "In these extraordinary times our government is taking extraordinary measures… Public health should never hinge on financial considerations."[108] Furthermore, Ontario's premier had also given his speech and made a promise to Ontarians that "We will do whatever it takes to protect and support the people of Ontario…in a way that is flexible and adaptable to

107. Ibid., 97; McCombs School of Business, "Cognitive Bias," Ethics Unwrapped, *The University of Texas at Austin,* 2023. Accessed on June 8, 2023, from https://ethicsunwrapped.utexas.edu/glossary/cognitive-bias
108. Trudeau, Justin, March 18, 2020, as cited in Rabson, Mia, "Trudeau promises $82B in economic supports in COVID-19 fight," *Toronto Star*, March 18, 2020, paras. 2-4. Accessed on June 8, 2023, from https://www.thestar.com/business/2020/03/18/morneau-to-unveil-20-billion-or-more-to-cushion-financial-shock-of-covid-19.html

changing circumstances…has informed the approach we are taking today…a plan that provides as much certainty as possible in an uncertain time...ensuring that we are always there to support those who need it most."[109] Moreover, they were told by Madan that his requests had come from the top and were highly confidential, in light of the COVID-19 situation that had no precedent; their such cognitive biases led to simply following what they were told.

Multifold, Incognito Communication in Cyberspace

When people are in unfamiliar circumstances like the pandemic, they may not act in their best interests, or they may but without their knowledge. For the Amazon cases, the unfair advantage could be realized because of the characteristics of its unique business model— two-sided, cross-border marketplace where buyers and sellers are interacting with each other, and sellers are competing against the other sellers in cyberspace and on a global scale. Buyers may not be using their formal names when purchasing products, whereas sellers may be advertising their products under different business names from time to time. Furthermore, product reviews can be posted by buyers who are masking their usernames. These people may also interact with Amazon employees remotely and globally for their various concerns and intent. Moreover, these transactions can be made through the use of virtual private network (VPN) and encrypted messaging services; at the end-user level (Layer 7 of the OSI model), these stakeholders can remain incognito unless the security systems are able to flag suspicious activities.

109. Ford, Doug, 2020, as cited in Phillips, Rod, 2020 Ontario Budget Speech, "Ontario's Action Plan," *Minister of Finance*, November 5, 2020, pp. 3-4. https://budget.ontario.ca/2020/pdf/2020-ontario-budget-speech-en.pdf

Investigation Perspectives

Auditor General

Since Madan was working within the ministry, the transactions performed under his role and responsibilities were to be examined and reported by the Auditor General of Ontario.[110] While it is uncertain as to how the Auditor General was doing their work in light of the COVID-19 pandemic, Madan's SFFP schemes were perpetrated during this time; the unusual protocols given to his subordinates were in fact used for cover, in addition to his own fraudulent activities. The Auditor General was either intricately conned or utterly not thorough at work. It appears that, since there had been no regular reporting or investigation (or little scrutiny) done by Ontario's auditors related to the domain of Madan's work until the discovery of his fraud schemes, both prevention and detection were not realistic; Madan was more thorough at his work with great attention to detail.[111] No new or better approach to their audit had been planned; it was revealed in consequence of the negative effects of overreliance on human judgment and existing control systems in place.[112]

110. Office of the Auditor General of Ontario, "2022 Annual Report," November 30, 2022. Accessed on June 9, 2023, from https://www.auditor.on.ca/en/content/annualreports/arbyyear/ar2022.html
111. Cohn, Martin Regg, "Doug Ford and the auditor general dropped the ball while a bureaucrat stole $47M," *Toronto Star*, April 18, 2023. Accessed on June 9, 2023, from https://www.thestar.com/politics/political-opinion/2023/04/18/doug-ford-and-the-auditor-general-dropped-the-ball-while-a-bureaucrat-stole-47m.html
112. Ibid., 33.

External Audit

FTX's financial statements used to be audited, according to FTX's claim.[113] Accounting rules such as the International Financial Reporting Standards (IFRS) had not explicitly referred to cryptocurrency; hence, professional accounting bodies have been in discussion for the determination of what rules of the existing standards should apply because each crypto asset has different terms and conditions.[114] While some crypto assets warrant an underlying good or service from an identifiable counterparty (the other party in investment trading), some crypto assets do not warrant any good or service and do not have any identifiable party.[115] Thus, crypto assets can be one of the following:

- Cash or cash equivalents
- Financial instruments (e.g., stocks, options, bonds, derivatives, etc.)
- Inventory
- Prepayments
- Intangible assets[116]

113. Foley, Stephen, "FTX collapse puts its auditors in the spotlight," *Financial Times*, November 13, 2022. Accessed on June 9, 2023, from https://www.ft.com/content/930c6cea-5457-4dfa-9d47-666c0698c335
114. McGulre, Rosemary, and Michael Massoud, "Introduction to accounting for cryptocurrencies under IFRS," *Chartered Professional Accountants (CPA) Canada*, May 2018. https://www.cpacanada.ca/-/media/site/operational/rg-research-guidance-and-support/docs/01713-rg-introduction-to-accounting-for-cryptocurrencies-may-2018.pdf; Ernst & Young, "Holdings of cryptocurrencies," IFRS Development, August 2019, Iss. 150. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-devel150-cryptocurrency-holdings-august-2019.pdf; Ernst & Young, "Applying IFRS Accounting by holders of crypto assets," October 2021. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-apply-ifrs-crypto-assets-update-october2021.pdf?download
115. Ibid., 114.
116. Ibid., 114.

As of October 2021, there are over 12,000 different cryptocurrencies in the world.[117] It is uncertain, as a private company, as to how FTX's crypto assets were treated for the accounting purposes. As mentioned above, crypto assets have diverse terms and conditions (hence, different accounting treatment required); however, some accounting firms are simply chasing opportunities, without adequate expertise, to get new clients from the growing crypto industry.[118] In addition, crypto laws and regulations are still unsettled in many parts of the world. After all, for the FTX case, there were many uncertainties as to what type of assurance engagement was conducted, what was the scope of that assurance engagement, and how extensively intercompany and intracompany transactions were scrutinized.[119] In the midst of such complexity and ambiguity, as of May 2023, only about a half of the top 60 crypto companies have been externally audited.[120]

117. Ibid., 114.
118. Ibid., 113; Ibid., 114.
119. Ibid., 113.
120. Ghosh, Monika, "Only half of top 60 crypto companies have an external auditor," *CryptoSlate*, May 15, 2023. Accessed on June 9, 2023, from https://cryptoslate.com/only-half-of-top-60-crypto-companies-have-an-external-auditor/

Investigative and Forensic Accounting (IFA) Practitioners' Roles

Roles and Responsibilities

The IFA practitioners are of independent and nonpartisan who are able to perform investigations objectively as free from a conflict of interest; in other words, they should not act as an advocate or be under the influence of any factors to exercise due diligence without bias.[121] They often provide expert evidence to court, by taking reasonable steps, to assist the judge and jury in decision-making; their primary duty is to court.[122]

The work of IFA is multidisciplinary in nature. Such practitioners may work at public accounting firms, consulting firms, financial institutions, insurance companies, public sectors, or the risk management, compliance, or internal audit department of various organizations with the following skillset:

- Problem identification, information gathering, and analytical skills
- Investigative and interviewing techniques
- Knowledge and experience of legal and court procedures
- Interpersonal and communication skills
- Attention to detail
- Background in auditing, accounting, law, psychology, criminology, information security, analytics, IT, computer forensics, etc.[123]

121. IFA Alliance, IFA Standards Committee, *Standard Practices for Investigative and Forensic Accounting Engagements*, Canadian Institute of Chartered Accountants (CICA), November 1, 2006; Crumbley, D. L., Fenton, E. D., and G. S. Smith, *Forensic and Investigative Accounting*, 9e, Riverwoods, IL: CCH Incorporated, 2019.
122. Ibid., 121.
123. Ibid., 121; ACFE, "Career Path Detail: Forensic Accountant," 2023. Accessed on June 9, 2023, from https://www.acfe.com/career/career-paths/career-path-accounting/career-path-detail-forensic-accountant

General

With the above skillset, the IFA practitioners specialize in conducting white-collar crime investigations. Therefore, they have knowledge of fraud schemes, typical characteristics of offenders, and relevant laws/regulations as well as the ability to recognize and analyze possible factors pertinent to the fraud diamond and assess internal controls and anomalies.[124] In addition, such a skill set might be applied to subcategories of the IFA domain such as loss quantification, business valuation, asset tracing/recovery, AML, and cybercrime investigations.[125]

Cybercrime-Related

Dealing with cybercrime investigations would need the knowledge of unique circumstances pertaining to cyberspace, cybercriminals, and incident response models.[126] In some cases, the IFA practitioners may team up with IT and/or AI professionals to uncover a particular scheme, especially for cyber-dependent crime.[127] Although humans' motivation and intent are still also concerned with cyber-dependent crime, bad actors' activities may only be active and visible within the IT infrastructure; furthermore, such activities and their identity and location might be masked by encryption, VPN, or spoofing for illicit system access, manipulation, interruption, and/or destruction.[128]

124. Ibid., 123.
125. Ibid., 123.
126. UNODC, "Who conducts cybercrime investigations?," Module 5: Cybercrime Investigation, March 2019. Accessed on May 20, 2023, from https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html
127. Ibid., 13; Ibid., 15.
128. Ibid., 21.

Approaches to Investigations

Mindset

Unlike auditors, the IFA practitioners do not rely on internal control systems or presume that people have integrity, rather maintaining a skeptical attitude.[129] With the ability to think like a criminal, they are able to picture where the weaknesses and opportunities are and how to exploit them.[130] Accordingly, they possess the investigative mindset and curiosity in identifying, tracking, analyzing, and evaluating relevant information.[131]

Processes

Each case that the IFA practitioners handle is unique; therefore, ingenious approaches to every investigation are required. Accordingly, the scope of work and required resources are different in every case.[132]

Once an engagement is accepted and signed after the discussion of client expectations and services to be rendered, the IFA practitioners start gathering data for analysis, while maintaining the chain of custody, in consideration of the scope of work and required resources determined for the particular investigation.[133] On occasion, it may not be possible to access information or reach out to particular individuals—identification and reporting of such limitations are necessary.[134] Thus, the ability to deal with

129. Ibid., 121.
130. "Successful Forensic Accountant Traits," *Financial Crime Academy*, 2023. Accessed on June 9, 2023, from https://financialcrimeacademy.org/successful-forensic-accountant-traits/
131. Ibid., 121; Ibid., 127.
132. Ibid., 123.
133. Ibid., 121.
134. Ibid., 121.

uncertainty is crucial to be able to make reasonable assumptions in best estimate and measure plausibility.[135]

During investigation, the IFA practitioners may need to consult wilt legal professionals or other experts on particular matters to choose the best or reasonable course of action and make inferences.[136] They are to have relevant documentation and evidence obtained in safekeeping while recording findings, references, discrepancies, and alternative theories as part of the evidence management and examination.[137]

Ultimately, the IFA practitioners report their findings, principles and methodologies employed, limitations impacted, underlying assumptions and rationale, and conclusions orally and/or in writing to relevant stakeholders—these may be provided to court and testified in person.[138]

Techniques/Tools

Regardless of the types of investigation, analysis, or review, the IFA practitioners need to undertake due diligence with an investigative mindset and professional skepticism, while having professional competence including accounting skills and investigative skills.[139] These techniques will effectively enhance the IFA practitioners' interviewing techniques that are necessary in order to gather relevant information.

In addition to the above, they often heavily rely on data analytics tools in processing a large amount of data obtained, which may be in different formats, and using

135. Ibid., 121.
136. Ibid., 121.
137. Ibid., 121.
138. Ibid., 121.
139. Ibid., 121; ACFE, "ACFE Code of Professional Ethics," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 2, 4.1002-4.1011.

data mining techniques to turn raw, unstructured data, through normalization, into useful and meaningful information.[140] In this process, they look into some recognizable patterns and anomalies to find clues and draw inferences through utilizing various functions such as filtering, stratifying, and summarizing data as well as detecting gaps and applying Benford's law, etc.[141] In combination, the automatic data extraction software, which comes with the optical character recognition (OCR) functionality, and data visualization tools may be used to improve the efficiency of document examinations and the accessibility to information.[142]

Implications Due to Technological Development

Emerging Issues

To this present day in our evolving data-driven world, Excel spreadsheets have been widely used by the IFA practitioners because of their familiarity and accessibility. However, they are not designed to import and analyze data from numerous heterogenous sources. In the age of big data, spreadsheets will no longer be able to efficiently deliver all the functionalities needed by the IFA practitioners for the fraud prevention and investigation purposes. The traditional techniques might still be manageable yet could be time-consuming and need an increased workforce. So, it is the time to ingest the growing

140. Ibid., 91.
141. Ibid., 91; CaseWare International Inc., "CaseWare IDEA Expanding the Audit Analytics Landscape," 2022. https://cms.caseware.com/wp-content/uploads/2023/04/cwi-idea-12-product-brochure-2022.pdf
142. Ibid., 91; IBM Cloud Education, "What Is Optical Character Recognition (OCR)?," *IBM Blog*, January 5, 2022. Accessed on June 9, 2023, from https://www.ibm.com/cloud/blog/optical-character-recognition

digital trend as fraud itself has also been ingesting the digital trend and growing into a different scale, especially with an increase in popularity of cryptocurrency transactions.[143]

Advantages. The basic principles of the risk management and investigations needed to combat against existing and emerging fraud are still the same—accounting skills, investigative skills, and an investigative mindset.[144] Yet, the incorporation of AI and machine learning (ML) can further support the prevention and detection of fraud such as identity thefts and account takeovers.[145] However, such AI/ML technologies and the endpoint detection and response (EDR) solution do not replace human intervention.[146] In other words, the human factors still play a significant role not only in perpetrating cybercrimes but also in intercepting such offenses because the systems and devices also still need to be configured, tested, and monitored by humans.[147] As the IFA practitioners, the amount of data will be more to process, analyze, and evaluate; however, the number of people required to conduct investigations may become fewer with the effective use of tools available and a strategic plan, which could be through a collaborative approach with other experts, according to the growing needs.

Disadvantages. The fraud cases related to cryptocurrency need the expertise in cryptocurrency, its relevant laws/regulations, and accounting rules because of its diversity and complexity, which depend on particular cryptocurrency's relevant geographic

143. Blake, Alex, "Cybercrime spiked in 2022 – and this year could be worse," *Digital Trends*, March 1, 2023. Accessed on June 9, 2023, from https://www.digitaltrends.com/computing/cybercrime-increased-in-2022-report/
144. Ibid., 121.
145. Ibid., 143.
146. IBM, "What is EDR (endpoint detection and response)?," n.d. Accessed on June 9, 2023, from https://www.ibm.com/topics/edr
147. Ibid., 5.

locations where certain laws/regulations apply.[148] Thus, in addition to the requirements of being tech savvy to a certain level, the IFA practitioners may need to put reliance on the work of or the information obtained from others experts in different industries.[149] Especially for cybercrimes, anonymization techniques are of great concerns that are possible through different means; looking into the system just for audit logs may need assistance from IT or cloud computing professionals, even though the IFA practitioners possess investigative skills and an investigative mindset.[150] If lacking technical knowledge or experience, they should not work beyond their expertise as the IFA practitioners.[151] When they need to engage with such technical experts, they should take reasonable steps to consider the nature and scope of reliance on those outsourced or collaborative work.[152]

Education and Professional Practice

Considerations for Future Exercises. As the number of cyber-related crime is growing, the role of the IFA practitioners will necessarily change in setting out strategies and plans such as timing, costs, scope, approach, techniques, tools, resources, and procedures of investigations. As the automation of repetitive tasks could be significantly optimized with the use of technology tools, the IFA practitioners will be able to put more time into focusing on other areas such as field investigations as well as the cross-examination of various source documents. The human-to-human aspects of investigations are the tasks that cannot be replaced by technology. Yet, with the effective

148. Ibid., 114.
149. Ibid., 114.
150. Ibid., 21; Ibid., 126.
151. Ibid., 121.
152. Ibid., 121.

use of technology, the IFA practitioners can gain a different level of insight when dealing with various sources of information in an attempt to make inferences or think of alternative theories. Hence, for the future IFA education and professional practice, more engagement with the technology related topics is encouraged, in addition to gaining the basic knowledge of information security in cyberspace.

Findings

The Most Vulnerable Area in the IT Infrastructure

The OSI model's Layer 7 is the most vulnerable; thus, it needs the strong IT governance and additional security controls in a layered approach, in consideration of the vulnerabilities of the other layers, since end-user interactions are the most significant at the application level. This is the most complex area to manage and where most of cyber-enabled crimes occur with the use of social engineering techniques. Because of significant human factors involved, this layer is not easy to prevent or mitigate cyberattacks only by strengthening networks and systems. Therefore, this is where the IFA practitioners' investigative skills and investigative mindset can be utilized.

The Significance of Cyber-Enabled Crime: Power

In looking into four cases, the most significant point was the fact that Madan (Ontario), Bankman-Fried (FTX), Kadimisetty (Amazon), and Rosenberg (Amazon) were playing God as if they would have held power over other people and organizations for the consequences of a series of events encompassing them. Furthermore, there are all four conditions of the fraud diamond met, which is an extension of the fraud triangle theory (opportunities, incentives, and rationalization plus the capacity factor), and all of them had collaborators.

Ongoing Ambiguity and Complexity of Crypto Assets

Things are happening in cyberspace, which is borderless. However, the IFA practitioners need to be cognizant of different legal and regulatory frameworks as well as different accounting treatment when it comes to cryptocurrency.

Recommendations

Due to the evolving situation related to cyber issues, while monitoring the standard setters' activities and guidance, the IFA practitioners should equip themselves with up-to-date knowledge and collaborate with experts in different disciplines (possibly forming cross-industry and cross-border) to deepen their understanding of unique circumstances pertinent to cyberspace, including developing digital currencies like crypto. Depending on the extent of cases involved, the IFA practitioners should also have adequate knowledge of relevant standards and regulatory and legal requirements in all relevant jurisdictions because of intricate differences in cyber-related issues.

The collaborative effort on a global scale is needed in consideration of the vulnerable factors from human, technological, legal, socioeconomic, and geographical perspectives as threat actors often try to break through multiple thrusted services through different methods of cyberattacks to execute their schemes.[153]

153. Ibid., 100; Detura, R., Ioshiura, C., Murphy, A., Richardson, B., Scheurle, S., Schweikert, E., and M. Vancauwenberghe, "A new approach to fighting fraud while enhancing customer experience," *McKinsey & Company*, November 8, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience#/

Conclusion

The more technology evolves, the more technology tools are utilized. The more technology evolves, the more opportunities for bad actors increase in cyberspace. The more technology evolves, the more security vulnerabilities are to be concerned. The more technology evolves, the more cybercrimes emerge. The more technology evolves, the more intricate social engineering techniques could become. The more technology evolves, the more experts are in need in various sectors, including the IFA practitioners.

The more complex emerging cybercrimes become, the more diverse knowledge and experience the IFA practitioners will need. The more complex emerging cybercrimes become, the more collaborative the IFA practitioners' work will be. The more complex emerging cybercrimes become, the more cognizant of cyberspace and cross-border issues the IFA practitioners need to be.

In conclusion, humans yet play a pivotal role both in perpetrating cybercrimes and in deterring or intercepting such offenses. Ultimately, this fast evolving situation affects the role and investigative techniques of the IFA practitioners. As the technology has changed the way of our communication and its systems and hence has enabled threat actors to emerge from anywhere without borders, the collaborative, global effort is encouraged in a multidisciplinary manner as a global concern. The IFA practitioners need to equip themselves with up-to-date knowledge to tackle the growing number of cybercrime in consideration of vulnerable factors from human, technological, legal, socioeconomic, and geographical perspectives. Keep your skepticism and investigative mindset towards cyberspace.

Bibliography

Albeda, Jouke, "Are IT General Controls Outdated? Data Protection and Internal Control Over Financial Reporting," *Information Systems Audit and Control Association (ISACA) Journal*, December 28, 2022, Vol. 6. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-6/are-it-general-controls-outdated

Allen, Lizzie, Press Center, "Amazon Marketplace a Winner for Customers, Sellers and Industry; New Service Grows over 200 Percent in First Four Months," *Amazon*, March 18, 2001. Accessed on May 27, 2023, from https://press.aboutamazon.com/2001/3/amazon-marketplace-a-winner-for-customers-sellers-and-industry-new-service-grows-over-200-percent-in-first-four-months

Amazon.com, Inc., *2022 Amazon Annual Report*, February 2, 2023. https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_AMZN_2022.pdf

"Amazon Japan returns $18m to suppliers in deal with Tokyo," *Nikkei Asia*, September 11, 2020. Accessed on June 8, 2023, from https://asia.nikkei.com/Business/Companies/Amazon-Japan-returns-18m-to-suppliers-in-deal-with-Tokyo

Andrieu, Thomas, "Crypto And FTX: The Return Of The Bank Run In The 21st Century," *GoldBroker*, November 15, 2022. Accessed on May 20, 2023, from https://goldbroker.com/news/cryptos-ftx-return-bank-run-21st-century-2915

Anonymous, as cited in Hadnagy, Christopher, "A Deep Dive Into Human Vulnerability," *Psychology Today*, May 15, 2022, para. 2. Accessed on June 5, 2023, from https://www.psychologytoday.com/ca/blog/human-hacking/202205/deep-dive-human-vulnerability

Arora, Gaurav, "Cryptoasset Regulatory Framework in Japan," *Social Science Research Network (SSRN)*, November 19, 2020. https://doi.org/10.2139/ssrn.3720230

Arsenych, Alex, "Former government employee pleads guilty to stealing $47.4-million from Ontario," *CTV News Toronto*, April 4, 2023. Accessed on May 18, 2023, from https://toronto.ctvnews.ca/former-government-employee-pleads-guilty-to-stealing-47-4-million-from-ontario-1.6342662

"ASGTG 2023," *ASGTG*, 2023. Accessed on June 3, 2023, from https://www.asgtg.com/event/asgtg-2023/

Associated Press, "The downfall of FTX's Sam Bankman-Fried sends shockwaves through the crypto world," *NPR*, November 14, 2022. Accessed on May 22, 2023, from https://www.npr.org/2022/11/14/1136482889/ftx-sam-bankman-fried-shockwaves-crypto

Association of Certified Fraud Examiners (ACFE), "Career Path Detail: Forensic Accountant," 2023. Accessed on June 9, 2023, from https://www.acfe.com/career/career-paths/career-path-accounting/career-path-detail-forensic-accountant

Association of Certified Fraud Examiners (ACFE), "Cyberfraud," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 1, 1.1401.

Association of Certified Fraud Examiners (ACFE), "Corruption," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 1, 1.625.

Association of Certified Fraud Examiners (ACFE), "Data Analysis and Reporting Tools," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 2, 3.701-3.749.

Association of Certified Fraud Examiners (ACFE), "ACFE Code of Professional Ethics," *Fraud Examiners Manual 2022 Edition: Financial transactions and fraud schemes, law, investigation, fraud prevention and deterrence*, 2021, Vol. 2, 4.1002-4.1011.

Berthiaume, Dan, "Exclusive: Amazon exec discusses how company is fighting online fraud," *Chain Store Age (CSA)*, December 1, 2022. Accessed on June 6, 2023, from https://chainstoreage.com/exclusive-amazon-exec-discusses-how-company-fighting-online-fraud

Berwick, A., Shiffman, J., and K. Gui Qing, "Exclusive: How a secret software change allowed FTX to use client money," *Reuters*, December 13, 2022. Accessed on June 8, 2023, from https://www.reuters.com/technology/how-secret-software-change-allowed-ftx-use-client-money-2022-12-13/

Bhole, Aneeta, "Sam Bankman-Fried's 'secret' $65 BILLION backdoor: FTX boss ordered co-founder to insert a single number into millions of lines of code to funnel clients' cash, attorneys claim," *Daily Mail*, January 14, 2023. Accessed on June 5, 2023, from https://www.dailymail.co.uk/news/article-11635721/Sam-

Bankman-Fried-ordered-FTX-founder-create-secret-backdoor-Alameda-Research.html

Blake, Alex, "Cybercrime spiked in 2022 – and this year could be worse," *Digital Trends*, March 1, 2023. Accessed on June 9, 2023, from https://www.digitaltrends.com/computing/cybercrime-increased-in-2022-report/

Bodoni, Stephanie, "Amazon Loses EU Court Fight Over Double Antitrust Sales Probes," *BNN Bloomberg,* April 20, 2023. Accessed on June 8, 2023, from https://www.bnnbloomberg.ca/amazon-loses-eu-court-fight-over-double-antitrust-sales-probes-1.1910031

Brown, Kimberly, Docket # 574, "List of Creditors (Verification of Creditors Matrix) Filed by FTX Trading Ltd.," Case 22-11068-JTD, Chapter 11, District of Delaware, United States Bankruptcy Court, January 25, 2023. https://document.epiq11.com/document/getdocumentbycode?docId=4142165&projectCode=FTX&source=DM

Canadian Centre for Cyber Security, "An introduction to the cyber threat environment," October 28, 2022. Accessed on May 14, 2023, from https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2023-2024," October 28, 2022. Accessed on May 14, 2023, from https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2023-2024

"Canadian Federal Court Rules Amazon Price-Fixing Case Will Go to Arbitration," *Competition Policy International (CPI),* October 13, 2022. Accessed on June 8,

2023, from https://www.competitionpolicyinternational.com/canadian-federal-court-rules-amazon-price-fixing-case-will-go-to-arbitration/

CaseWare International Inc., "CaseWare IDEA Expanding the Audit Analytics Landscape," 2022. https://cms.caseware.com/wp-content/uploads/2023/04/cwi-idea-12-product-brochure-2022.pdf

Chee, Foo Yun, "Amazon may face EU antitrust charges over merchant data in coming weeks: source," *Reuters*, June 11, 2020. Accessed on June 8, 2023, from https://www.reuters.com/article/us-eu-amazon-com-antitrust-idCAKBN23I2V7

Chee, Foo Yun, "Amazon settlement with EU antitrust regulators possible by year end - sources," *Reuters*, November 25, 2022. Accessed on June 8, 2023, from https://www.reuters.com/technology/amazon-settlement-with-eu-antitrust-regulators-possible-by-year-end-sources-2022-11-25/

Cohn, Martin Regg, "Doug Ford and the auditor general dropped the ball while a bureaucrat stole $47M," *Toronto Star*, April 18, 2023. Accessed on June 9, 2023, from https://www.thestar.com/politics/political-opinion/2023/04/18/doug-ford-and-the-auditor-general-dropped-the-ball-while-a-bureaucrat-stole-47m.html

"Contact Ed," *ASGTG*, n.d. Accessed on June 3, 2023, from https://www.asgtg.com/contact/

Council of the European Union, Press Release, "Digital finance: Council adopts new rules on markets in crypto-assets (MiCA)," May 16, 2023. https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/digital-finance-council-adopts-new-rules-on-markets-in-crypto-assets-mica/

Crown Prosecution Service, Legal Guidance, "Cybercrime - prosecution guidance," September 26, 2019. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Crumbley, D. L., Fenton, E. D., and G. S. Smith, *Forensic and Investigative Accounting*, 9e, Riverwoods, IL: CCH Incorporated, 2019.

"Cryptocurrency regulation diverges across Asia," *Economist Intelligence Unit (EIU)*, February 8, 2022. Accessed on May 23, 2023, from https://www.eiu.com/n/cryptocurrency-regulation-diverges-across-asia/

Deposit Insurance Corporation (DIC) Bahamas, "Who are DIC Member Institutions?," December 23, 2022. Accessed on May 22, 2023, from https://www.dic.bs/di-members.php

Detura, R., Ioshiura, C., Murphy, A., Richardson, B., Scheurle, S., Schweikert, E., and M. Vancauwenberghe, "A new approach to fighting fraud while enhancing customer experience," *McKinsey & Company*, November 8, 2022. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience#/

D'Mello, Colin, "Former Ontario government employee pleads guilty to multi-million dollar fraud," *Global News*, April 4, 2023. Accessed on May 18, 2023, from https://globalnews.ca/news/9601082/former-ontario-government-employee-guilty-plea-multi-million-dollar-fraud/

Elder, Bryce, and Alexandra Scaggs, "The FTX bankruptcy filing in full (updated)," *Financial Times*, November 17, 2022. Accessed on May 20, 2023, from https://www.ft.com/content/c236d6f9-da5a-4da7-8dc8-5cd450dfe39d

Emerson, Sarah, "FTX Owes Money To Every Major Tech Company, Including Google, Meta, Amazon And Apple," *Forbes*, January 26, 2023. Accessed on May 20, 2023, from https://www.forbes.com/sites/sarahemerson/2023/01/26/ftx-owes-money-to-every-major-tech-company-google-meta-amazon-tiktok-apple/

Epiq Systems, Inc., "FTX Trading Official Committee of Unsecured Creditors," Case # 22-11068, November 11, 2022. Accessed on May 23, 2023, from https://dm.epiq11.com/case/ftx/info

Ernst & Young, "Holdings of cryptocurrencies," IFRS Development, August 2019, Iss. 150. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-devel150-cryptocurrency-holdings-august-2019.pdf

Ernst & Young, "Applying IFRS Accounting by holders of crypto assets," October 2021. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ifrs/ey-apply-ifrs-crypto-assets-update-october2021.pdf?download

European Commission (EC), Press Release, "Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime," December 20, 2022. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777

European Commission (EC), "Cybercrime," *Directorate-General for Migration and Home Affairs*, n.d. Accessed on May 21, 2023, from https://home-affairs.ec.europa.eu/cybercrime_en

European Parliament, Press Releases, "Crypto-assets: green light to new rules for tracing transfers in the EU," April 20, 2023.

https://www.europarl.europa.eu/news/en/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu

European Union Agency for Cybersecurity, “What is ‘Social Engineering’?,” 2023. Accessed on May 20, 2023, from https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

European Union Agency for Network and Information Security, “Cyber Security Culture in organisations,” November 2017. https://doi.org/10.2824/10543

Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2016,” December 6, 2021. https://doi.org/10.2813/275589

Europol, “The Internet Organised Crime Threat Assessment (IOCTA) 2018,” January 11, 2019. https://doi.org/10.2813/858843

Evans, Pete, “‘I didn't ever try to commit fraud on anyone,’ FTX founder Sam Bankman-Fried says,” *CBC News*, November 30, 2022. Accessed on June 5, 2023, from https://www.cbc.ca/news/business/ftx-sam-bankman-fried-1.6669767

Federal Deposit Insurance Corporation (FDIC), Fact Sheet, “What the Public Needs to Know About FDIC Deposit Insurance and Crypto Companies,” July 28, 2022. https://www.fdic.gov/news/fact-sheets/crypto-fact-sheet-7-28-22.pdf

Federal Deposit Insurance Corporation (FDIC), Press Releases, “Potential Violations of Section 18(a)(4) of the Federal Deposit insurance Act,” August 18, 2022. https://www.fdic.gov/news/press-releases/2022/ftx-harrison-letter.pdf

Financial Services Agency (FSA) 金融庁, Policy, “Summary of the Systematization of Legal Infrastructure Related to Crypto Assets 暗号資産（仮想通貨）に関連す

る制度整備について," April 7, 2021.

https://www.fsa.go.jp/policy/virtual_currency/20210407_seidogaiyou.pdf

"FTX - Crunchbase Investor Profile & Investments," *Crunchbase*, 2023. Accessed on May 20, 2023, from https://www.crunchbase.com/organization/ftx-exchange

"FTX (FTT): Its Downfall & The Launch of FTX 2.0," *Bybit Learn*, May 29, 2023. Accessed on June 1, 2023, from https://learn.bybit.com/crypto/what-is-ftt/

Foley, Stephen, "FTX collapse puts its auditors in the spotlight," *Financial Times*, November 13, 2022. Accessed on June 9, 2023, from https://www.ft.com/content/930c6cea-5457-4dfa-9d47-666c0698c335

Ford, Doug, 2020, as cited in Phillips, Rod, 2020 Ontario Budget Speech, "Ontario's Action Plan," *Minister of Finance*, November 5, 2020, pp. 3-4. https://budget.ontario.ca/2020/pdf/2020-ontario-budget-speech-en.pdf

Fuje, H., Quayyum, S., and T. Molosiwa, Blog, "Africa's Growing Crypto Market Needs Better Regulations," *IMF*, November 22, 2022. Accessed on May 23, 2023, from https://www.imf.org/en/Blogs/Articles/2022/11/22/africas-growing-crypto-market-needs-better-regulations

Ghosh, Monika, "Only half of top 60 crypto companies have an external auditor," *CryptoSlate*, May 15, 2023. Accessed on June 9, 2023, from https://cryptoslate.com/only-half-of-top-60-crypto-companies-have-an-external-auditor/

Gibbs, Samuel, "Amazon's Japanese headquarters raided by nation's regulator," *The Guardian*, March 15, 2018. Accessed on June 8, 2023, from

https://www.theguardian.com/technology/2018/mar/15/amazon-japanese-headquarters-raided-regulator-antitrust-fair-trade-commission

Goel, S., Williams, K., and E. Dincelli, "Got Phished? Internet Security and Human Vulnerability," *Journal of the Association for Information Systems (JAIS)*, January 31, 2017, Vol. 18, Iss. 1, 22-44. https://doi.org/10.17705/1jais.00447

Gomzin, Slava, *Crypto Basics: A Nontechnical Introduction to Creating Your Own Money for Investors and Inventors*, 1e, Berkeley, CA: Apress, 2022. https://doi.org/10.1007/978-1-4842-8321-9

Hadnagy, Christopher, "A Deep Dive Into Human Vulnerability," *Psychology Today*, May 15, 2022. Accessed on June 5, 2023, from https://www.psychologytoday.com/ca/blog/human-hacking/202205/deep-dive-human-vulnerability

Hetler, Amanda, "FTX scam explained: Everything you need to know," *TechTarget*, April 17, 2023. Accessed on May 20, 2023, from https://www.techtarget.com/whatis/feature/FTX-scam-explained-Everything-you-need-to-know

His Majesty the King in Right of Ontario v. Madan, 2022 ONSC 5355 (CanLII). https://canlii.ca/t/js0pv

His Majesty the King in Right of Ontario v. Madan, 2023 ONSC 2831 (CanLII). https://canlii.ca/t/jx6tg

Her Majesty the Queen in Right of Ontario v. Madan, 2022 ONSC 5103 (CanLII). https://canlii.ca/t/jrt19

Her Majesty the Queen in Right of Ontario v. Madan et al., 2022 ONSC 1538 (CanLII). https://canlii.ca/t/jn5xk

HMQ v. Madan, 2020 ONSC 8093 (CanLII). https://canlii.ca/t/jcr9t

House of Commons, Evidence, "Standing Committee on Industry, Science and Technology," May 20, 2020, Number 016, 43rd Parliament, 1st Session. https://www.ourcommons.ca/Content/Committee/431/INDU/Evidence/EV10761671/INDUEV16-E.PDF

"How Amazon Seller's Group Began," *Amazon Sellers Group TG (ASGTG)*, n.d. Accessed on June 3, 2023, from https://www.asgtg.com/about/

IBM, "The Fundamentals of Networking," n.d. Accessed on May 14, 2023, from https://www.ibm.com/topics/networking

IBM, "What is EDR (endpoint detection and response)?," n.d. Accessed on June 9, 2023, from https://www.ibm.com/topics/edr

IBM Cloud Education, "What Is Optical Character Recognition (OCR)?," *IBM Blog*, January 5, 2022. Accessed on June 9, 2023, from https://www.ibm.com/cloud/blog/optical-character-recognition

IFA Alliance, IFA Standards Committee, *Standard Practices for Investigative and Forensic Accounting Engagements*, Canadian Institute of Chartered Accountants (CICA), November 1, 2006.

International Organization for Standardization, "ISO/IEC 7498-1:1994(en) Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model – Part 1," November 15, 1994. https://www.iso.org/obp/ui/#iso:std:iso-iec:7498:-1:ed-1:v2:en

Irwin, Kate, "Sam Bankman-Fried Says FTX Hacker May Be a Former Employee," *Decrypt,* November 29, 2022. Accessed on June 5, 2023, from https://decrypt.co/115963/sam-bankman-fried-ftx-hacker-former-employee

Japan Fair Trade Commission (JFTC), Press Releases, "Approval of the Commitment Plan submitted by Amazon Japan G.K.," September 10, 2020. https://www.jftc.go.jp/en/pressreleases/yearly-2020/September/200910.html

Key, Alys, "Chainalysis Confirmed as FTX Creditor in Bankruptcy Case," *Decrypt,* November 17, 2022. Accessed on May 22, 2023, from https://decrypt.co/114931/chainalysis-confirmed-ftx-creditor-bankruptcy-case

Kolhatkar, Sheelah, "How Serious Are Sam Bankman-Fried's Alleged Campaign-Finance Violations?," *The New Yorker,* January 11, 2023. Accessed on May 24, 2023, from https://www.newyorker.com/business/currency/how-serious-are-sam-bankman-frieds-alleged-campaign-finance-violations

Lou, Ethan, "Easy Money: The scam that revealed chaos and a culture of fraud at Queen's Park," *Toronto Life,* May 25, 2021. Accessed on May 20, 2023, from https://torontolife.com/city/the-scam-that-revealed-chaos-and-a-culture-of-fraud-at-queens-park/

McCombs School of Business, "Cognitive Bias," Ethics Unwrapped, *The University of Texas at Austin,* 2023. Accessed on June 8, 2023, from https://ethicsunwrapped.utexas.edu/glossary/cognitive-bias

McGulre, Rosemary, and Michael Massoud, "Introduction to accounting for cryptocurrencies under IFRS," *Chartered Professional Accountants (CPA) Canada,* May 2018. https://www.cpacanada.ca/-/media/site/operational/rg-

research-guidance-and-support/docs/01713-rg-introduction-to-accounting-for-cryptocurrencies-may-2018.pdf

Mello-Klein, Cody, "Amazon is transforming what a small business is–and it looks just like Amazon. Is that a good thing?," *Northeastern Global News*, January 27, 2023. Accessed on May 27, 2023, from https://news.northeastern.edu/2023/01/27/amazon-small-business-transformation/

Microsoft, "What is an endpoint?," *Microsoft Security*, 2023. Accessed on May 20, 2023, from https://www.microsoft.com/en-ca/security/business/security-101/what-is-an-endpoint

Narain, Aditya, and Marina Moretti, Publications, "Regulating Crypto," *International Monetary Fund (IMF)*, September 2022. https://www.imf.org/en/Publications/fandd/issues/2022/09/Regulating-crypto-Narain-Moretti

Office of the Auditor General of Ontario, "2022 Annual Report," November 30, 2022. Accessed on June 9, 2023, from https://www.auditor.on.ca/en/content/annualreports/arbyyear/ar2022.html

Office of the Superintendent of Financial Institutions (OSFI), Statement, "Statement to entities engaging in crypto-asset activities or crypto-related services," November 16, 2022. https://www.osfi-bsif.gc.ca/Eng/osfi-bsif/med/Pages/20221116_let.aspx

Organisation for Economic Co-operation and Development (OECD), United Nations Office on Drugs and Crime (UNODC), World Bank, "Anti-Corruption Ethics and Compliance Handbook for Business," 2013. https://www.oecd.org/corruption/anti-corruptionethicscompliancehandbook.pdf

Palmer, Annie, "DOJ charges six people in scheme to bribe Amazon employees to 'gain upper hand' on marketplace," *CNBC,* September 18, 2020. Accessed on May 27, 2023, from https://www.cnbc.com/2020/09/18/doj-charges-six-people-in-scheme-to-bribe-amazon-employees.html

Palmer, Annie, "Former Amazon employee sentenced to 10 months in prison for involvement in bribery scheme," *CNBC,* February 11, 2022. Accessed on May 27, 2023, from https://www.cnbc.com/2022/02/11/former-amazon-employee-sentenced-to-10-months-in-bribery-scheme.html

Palmer, Annie, "Amazon seller consultant admits to bribing employees to help clients; will plead guilty," *CNBC,* March 27, 2023. Accessed on June 3, 2023, from https://www.cnbc.com/2023/03/27/amazon-seller-consultant-admits-to-bribing-employees-to-help-clients.html

Perkel, Colin, The Canadian Press, "'I felt betrayed': Family denies helping father who allegedly stole $11M in Ontario COVID relief," *National Post,* January 26, 2021. Accessed on May 18, 2023, from https://nationalpost.com/news/canada/civil-servant-betrayed-family-with-alleged-11-million-covid-relief-fraud-docs

Regulated United Europe (RUE), "Crypto Regulations in Switzerland," 2023. Accessed on May 23, 2023, from https://rue.ee/crypto-regulations/switzerland/

Rosenberg, Ed, [Amazon Sellers Group TG], *Apology From Ed Rosenberg.* [Video], YouTube, March 27, 2023, paras. 2-3. Accessed on June 3, 2023, from https://www.youtube.com/watch?v=v410zJ46Mpk

Rosenberg, Ed, [Amazon Sellers Group TG], *EU Kyc Funds Held FBA Blocked Company Address Verification Issue. Great Info For Amazon* [Video], YouTube,

May 22, 2023. Accessed on June 3, 2023, from https://www.youtube.com/watch?v=AxTg7GBUy6k

Royal Canadian Mounted Police, News Release, "Fraud Prevention Month 2023: Fraud losses in Canada reach another historic level," February 27, 2023. https://www.rcmp-grc.gc.ca/en/news/2023/fraud-prevention-month-2023-fraud-losses-canada-reach-historic-level

Scannell, Kara, and Allison Morrow, "Sam Bankman-Fried wants his case thrown out of court," *CNN Business*, May 8, 2023. Accessed on May 22, 2023, from https://www.cnn.com/2023/05/08/tech/sbf-ftx-dismissal-hnk-intl/index.html

Securities and Exchange Commission, Plaintiff, v. Nishad Singh, Defendant, Case 1:23-cv-01691, Southern District of New York, United States District Court, February 28, 2023, para. 5. https://www.sec.gov/litigation/complaints/2023/comp25652.pdf

Securities Commission of the Bahamas, Media Release, "IOSCO Sets the Standard for Global Crypto Regulation," *International Organization of Securities Commissions (IOSCO)*, May 23, 2023. https://www.scb.gov.bs/wp-content/uploads/2023/05/IOSCONEWS693.pdf

Silverman, Sam, "From Tom Brady to Kevin O'Leary - See Who Lost Big in the Wake of the FTX Crypto Collapse," *Entrepreneur*, January 25, 2023. Accessed on May 20, 2023, from https://www.entrepreneur.com/business-news/who-lost-money-in-ftx-tom-brady-kevin-oleary-and-more/443653

Sisco, Josh, "Washington prepares for war with Amazon," *Politico*, March 20, 2023. Accessed on June 8, 2023, from https://www.politico.com/news/2023/03/20/ftc-amazon-irobot-antitrust-00087711

Smith, Jonathan, "Biotech Startups Face a Growing Wave of Cyberattacks," *Labiotech*, June 25, 2022. Accessed on May 14, 2023, from https://www.labiotech.eu/in-depth/cyberattack-biotech-startups-covid/

Star Editorial Board, "The security lapse that cost Ontario taxpayers," *Toronto Star*, April 14, 2023. Accessed on May 20, 2023, from https://www.thestar.com/opinion/editorials/2023/04/14/the-security-lapse-that-cost-ontario-taxpayers.html

State Secretariat for International Finance (SIF), "Blockchain / DLT," December 23, 2022. Accessed on May 23, 2023, from https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html

Steiner, Ina, "Well Known Amazon Consultant to Plead in Bribery Case," *EcommerceBytes*, March 25, 2023. Accessed on June 3, 2023, from https://www.ecommercebytes.com/2023/03/25/well-known-amazon-consultant-to-plead-in-bribery-case/

"Successful Forensic Accountant Traits," *Financial Crime Academy*, 2023. Accessed on June 9, 2023, from https://financialcrimeacademy.org/successful-forensic-accountant-traits/

Swanson, Scott, "The role of fraud examinations in cybercrime," *Fraud Magazine*, August 2015. https://www.fraud-magazine.com/article.aspx?id=4294989368

Trudeau, Justin, March 18, 2020, as cited in Rabson, Mia, "Trudeau promises $82B in economic supports in COVID-19 fight," *Toronto Star*, March 18, 2020, paras. 2-4. Accessed on June 8, 2023, from

https://www.thestar.com/business/2020/03/18/morneau-to-unveil-20-billion-or-more-to-cushion-financial-shock-of-covid-19.html

Turay, Brima, "Analysis of Seven Layered Architecture of OSI Model," *Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS),* December 13, 2019, Vol. 2, Iss. 12, 73-77. https://ssrn.com/abstract=3815237

United States Attorney's Office, Western District of Washington, Press Release, "First of six consultants indicted in Amazon bribery scheme sentenced to prison," *U.S. Department of Justice (DOJ),* February 11, 2022. https://www.justice.gov/usao-wdwa/pr/first-six-consultants-indicted-amazon-bribery-scheme-sentenced-prison

United States of America, Plaintiff, v. Ephraim Rosenberg and Hadis Nuhanovic, Defendant, Case 2:20-cr-00151-RAJ, Western District of Washington, United States District Court, July 18, 2022. https://casetext.com/case/united-states-v-rosenberg-51

United Nations Office on Drugs and Crime (UNODC), "Who conducts cybercrime investigations?," Module 5: Cybercrime Investigation, March 2019. Accessed on May 20, 2023, from https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html

United Nations Office on Drugs and Crime (UNODC), "Global Programme on Cybercrime," n.d. Accessed on May 21, 2023, from https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

U.S. Securities and Exchange Commission (SEC), Litigation Release No. 25616, "Securities and Exchange Commission v. Samuel Bankman-Fried, No. 1:22-cv-

10501 (S.D.N.Y. filed Dec. 13, 2022)," January 19, 2023. https://www.sec.gov/litigation/litreleases/2023/lr25616.htm

U.S. Securities and Exchange Commission (SEC), "Ponzi Scheme," *Investor.gov*, n.d. Accessed on May 24, 2023, from https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme

Ursillo, Steve, Jr., and Christopher Arnold, "Cybersecurity Is Critical for all Organizations – Large and Small," *International Federation of Accountants*, November 4, 2019. Accessed on May 15, 2023, from https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small

Verma, Raina, "How Fraudsters Exploit the Capabilities of Contract Employees to Conduct Their Schemes," *ACFE Insights*, July 28, 2021. Accessed on June 4, 2023, from https://www.acfeinsights.com/acfe-insights/how-fraudsters-exploit-the-capabilities-of-contract-employees-to-conduct-their-schemes

Wang, Z., Sun, L., and H. Zhu, "Defining Social Engineering in Cybersecurity," *Institute of Electrical and Electronics Engineers (IEEE) Access*, May 19, 2020, Vol. 8, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

Warren, Elizabeth, Press Releases, "Warren, Marshall Introduce Bipartisan Legislation to Crack Down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations," *U.S. Senator Elizabeth Warren of Massachusetts*, December 14, 2022. https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations

"What are the 7 layers of the OSI model?," *DataDome*, October 24, 2021. Accessed on May 14, 2023, from https://datadome.co/learning-center/7-layers-osi-model/

"What is Ethereum?," *ethereum.org*, 2023. Accessed on June 1, 2023, from https://ethereum.org/en/what-is-ethereum/

Zhuo, S., Biddle, R., Koh, Y. S., Lottridge, D., and G. Russello, "SoK: Human-centered Phishing Susceptibility," *Association for Computing Machinery (ACM) Journal*, April 14, 2023, Vol. 26, Iss. 3, Article 24, 1-27. https://doi.org/10.1145/3575797