AI, a Provenance or Solution for Financial Crime

***Suzan Dsouza, Houshang Habibniya, Rezart Demiraj**
Accounting Department, College of Business Administration, American University of the Middle East, Kuwait.

***Correspondence:** suzan.dsouza@aum.edu.kw

Received: May 05, 2021; Accepted: Jun 28, 2021

CITATION: Dsouza S, Habibniya H, Demiraj R. 2021. AI, a Provenance or Solution for Financial Crime. Management and Economics Research Journal, 7(2): 1-5, Article ID 1423084. DOI: 10.18639/MERJ.2021.1423084

ABSTRACT
This article consists a review of the existing literature on artificial intelligence (AI) with respect to financial crimes. The purpose is to notify the unintentional bad impacts and intentional good impacts of AI applications in relation to financial crimes. This article has reinforced the discussions stating AI applications to be considered as a solution for financial crimes instead of being criticized as the cause for financial crime. The public and private sectors both need be alert with the unintentional harm caused by cybercrime. The current behavior of AI is considered as an accelerator or an antidote to financial crimes, specific to cybercrimes. It is advised to apply criminal law to control cybercrimes. However, holding the AI agents responsible is considered to be an inappropriate mechanism. Thus, AI systems are still not deemed to be capable of forming a proper legitimate system in order to curb the financial crimes.

KEYWORDS: Cybercrime; Financial Crime; Fraud; Artificial Intelligence (AI).

1. INTRODUCTION

The modern artificial intelligence (AI) was originally founded by computer scientists in the 1950s. It is an artificial system that can perform various tasks under such environment that can vary but cannot be unpredictable. These tasks are performed with minimum human interference. Today AI is a multidisciplinary field with applications in nearly every aspect of human life.

The evolution of AI has termed the systems to act and think like humans with rational thinking power or with rational actions. The AI systems solve tasks that may need human-like planning, learning, perception, communication, cognition, or physical actions (Hoadley and Lucas, 2018). Progression and application of AI systems are ideally considered as a boon for economic growth and overall productivity (Furman and Seamans, 2018). As emerging algorithm-driven AI continues to spread, multiple myths have been set. The most common is the idea that the existence of AI can lead to a long-term threat to mankind. This has been characterized to be as the most pervasive myth which in turn has developed numerous misinterpretations and fears about AI systems (Bentley *et al.*, 2018). There are, however, genuine worries regarding the AI systems to be a threat to the society which includes continuation of financial crimes (Forwood and Bolton, 2018). Almost every economy across the world is a victim of financial crime. This increasingly sophisticated and global issue of financial crime has profound implications on individuals, organizations, businesses, and government agencies in both developed and developing countries. Despite of various countermeasures and global collaborative approaches, very few countries are able to partially survive out of the caused crises. Unfortunately, financial crime has gained global popularity with the AI system support.

2. NATURE AND SIGNIFICANCE OF FINANCIAL CRIMES

Financial crimes or economic crimes in general refer to such criminal acts which are nonviolent in nature but they result in financial losses to the victims (IMF, 2001). It is also termed as any illegal action performed by an individual entity or groups of individuals, where the indication is to acquire a professional or financial gain from a perpetrator's perspective. The terms financial abuse and financial crime are far less precise, and in fact are sometimes used interchangeably. The National Crime Agency explains financial crimes as economic crimes under the context ranging from tax evasion, money laundering, counterfeit currency, and corruption. However, these acts lead to misuse of the economic aid. Gottschalk (2010) explained financial crimes under four main categories. i) corruption, ii) fraud, iii) theft, and iv) manipulation. Corruption would include embezzlement, bribery, kickbacks, and extortion. Fraud can be a human character. However, theft can be of cash or intellectual property, and manipulation can happen with acts like bid rigging, cybercrime, money laundering, and insider trading. It is very difficult to determine the overall phenomenon. It is recognized as a portion of absence in clarity and accepted concepts which are later provoked by systems that report across various global economies (Treasury Committee, 2018; UNODC, 2005). However, there is no definition for financial crime which has international acceptance (Treasury Committee, 2018; Ryder, 2011). In order to avoid

semantical arguments, the economic crimes are interchangeably used, considering the views which could limit the perception to crimes occurred in the financial and capital markets (Frunza, 2016).

Pickett and Pickett (2002) explained financial crimes to be as practicing dishonesty in order to have illegal gains that generally happen due to breach of faith with some concealment of activities which seem to be true. Financial crime is considered generally to be global as there is an extensive arrangement undertaken through Internet networks. By the fundamentals, international crimes and cybercrime are connected to financial crimes. They have harmful implications on individuals and financial institutions all over the world. The stakeholders to financial, telecom, and legal industrial sectors will have to collaborate to find a solution to this threat. Financial crimes are popular to be international and digital in nature (Jung and lee, 2017; Ryder *et al*., 2014). The first reason is to have illegal financial gain and to bypass the vigilance of local enforcement and legal agencies. The second reason is the speed; digital transactions generally occur within fraction of seconds which regrettably skip the sensor of customs inspection. This is one of the main reasons why digital money is the most popular in financial crimes. However, this was made possible and expedited by the advent of information technology (Castells and Cardoso, 2005), and later supported by the block chain systems (Everette, 2017; Brown, 2016). The negative implications of 2007 global financial crisis continue on many economies across the globe, caused by financial crimes (Ryder *et al*., 2014). The growing business modes supported with constant upgrades in technology have resulted cyber platform to be the core tool used by criminals to perform different levels of financial crimes. The core impact of technology has been on industries which process and comply with financial transactions, for instance, industrial sectors where the major control is held by financial institutions, including the insurance sector, the banking entities, retail sectors, etc. This may be considered as a strong and ever growing indication of emergent combination of financial with cybercrimes (McGuire, 2012). It is later stated to be the main reason to bridge the gap between the independent domains of fraud and compliance with the cyber security and intelligence (Macaulay, 2017).

The actual cause of economic crimes and the way it affected businesses across the world was a subject of an in-depth survey analysis undertaken by a researcher (Bussmann, 2007). The report revealed the worldwide persistence of fraud. This occurred despite of strict controls and vigilance placed by the concerned authorities. The actual economic crimes and their related financial and nonfinancial implications have not reduced. Almost 50% of the businesses were victimized to economic crime between 2006 and 2007. The survey respondents reported a total loss of more than USD 4.2 billion. Considering the businesses with weaker control systems, the total estimated losses would, however, exceed USD 5.7 billion (Bussmann, 2007). The survey concluded that the most significant types of economic crimes are accounting fraud, intellectual property infringements, corruption and bribery, money laundering, and asset misappropriation. It was also observed that no sufficient fraud control measures were adapted. It was suggested that corporate cultural ethics could play a supportive role in preventing fraudulent activities in such organizations. The survey also states some of the difficulties and unmanageable situations to avoid complete economic crimes. Some of the success measures and shortcomings observed in combating against economic crimes were also discussed in the report which later may serve as a relevant literature for future decision-making.

The Global Economic and Fraud survey held in 2018 concluded that though there is rising awareness related to the threats caused by economic crimes, the reality shows awareness with very few business entities that were completely aware of the risk faced by them (Lavion *et al*., 2018). The survey indicated an increase of 13% from 2016 to 2018 in corporate victims caused by economic crimes and frauds. There frauds were reported across all industries. The victims targeted ranged from financial services, professional services, consumer, industrial and technology involved in bribery to corruption, consumer and procurement frauds, money laundering, business misconduct, cybercrime, and asset misappropriation. Consumer fraud, cybercrime, and asset misappropriation were reported as the top most crime categories. The report yet identified cybercrime as threat with high probability of occurrence for the next 2 years. Despite of a surge in cost of preventing measures against criminal incursions into the financial systems, financial crime across the globe continued. Thus, there can be recognition to awareness of growing fraudulent activities around the world, leading to better clarity on the involved fraudulent actions, followed by the required data capture, pool of big data, and the applied big data analytics. It is fascinating to note that the corporate internal stakeholders like senior managements constitute nearly 24% of the total economic crimes committed. The external stakeholders like customers shared service providers, vendors, and agents accounted for 68% of these crimes.

Apart from the monetary losses, economic crimes had a huge negative impact on the reputation/brand strength, relations with regulators, share valuations for listed entities, employee morale, and business relations. It is vital to note the supporting role of AI to technologies and financial services in preventing occurrence of economic crimes. These relate to predictive analytics, machine learning, voice recognition, natural language processing, and natural language generation (Lavion *et al*., 2018).

However, this gives an explanation to why financial service entities, bank, and public institutions consider the fight against crime to be as a priority. Unfortunately, AI supported by other technologies acts as a support to enable financial crime encouraging an online rise of sophisticated culprits. The reality states AI to be the ever strongest tool which the society needs to defeat (Craig, 2018). These threats can be nailed if the public and private organizations work together against these fears.

3. CYBERCRIME

Cybercrime is a highly influential terminology, holding a huge population as victims. Millions of people globally are victimized with theft of their personal information or compromised. One of the main reasons for growth in cybercrime may be attributed to

a speedy adoption of latest technology undertaken by the cybercriminals. Low-income economies with a weak cyber security having increased population of online users may also be considered as the major cause of cybercrimes. The other additional factors which presume to be part of cybercrimes are i) rising and expanding horizon of cybercrimes hotspots, ii) growing sophistication amid the cybercriminals who belong to the top-tier category, iii) increasing the use of digital currencies across the globe, and iv) propagation of Dark Web. The Dark Web, which uses masked IP addresses, is capable of creating transactions with high complexity that may involve further stakeholders like brokers and other agents in the black markets. A trend rate of growth in cybercrime has been predicted. The hackers are continuously in the business of Internet manipulation by targeting security weakness and compromising vulnerable devices to conduct cyberattacks through sophisticated use of AI tools. They create high level of malware and cause infections via interventions into the cloud. The cybercrime may well be characterized as a financial threat by linking it to the Internet economy, which is globally expanding at a rapid pace. Among other sectors, banks have always been the most attractive targets for such skillful cyber criminals. Thus, the most undiversifiable risk to the financial stability of the economy is caused by financial crimes. The most popular countries with rising frequency in hacking of financial institution data are Russia, North Korea, and Iran (France-Presse, 2018).

The national governmental institutions may play a critical role in preventing criminal hackers through sound laws and regulations and by helping quickly address a large cyber event before it becomes a national or global crisis. Governments may also help improve the public–private cybersecurity workforce through training programs and sharing of cybersecurity information. Cybercrime and frauds committed online are the most regular crimes in the United Kingdom consisting of millions annual offences. These could cover almost half of the criminal offences across the country. Various well-coordinated initiatives are vital to be implemented on a global level. They may include i) mutual supportive cooperation among international law enforcements, ii) mutual amendments and improvements to the prevailing Mutual Legal Assistance Treaty, iii) well-developed data collection processes, iv) application of primary security measures, v) well-invested defensive technologies, vi) well-structured, vii) and systematic implementation of cyber security (Lewis, 2018). The international legal system like the International Criminal Court must adapt to this battleground to force the failing countries be financially accountable.

4. ARTIFICIAL INTELLIGENCE IN CYBERCRIME

AI is expected to play an important role in future in relation to criminal acts. Artificial Intelligence Crime explains the occurrence of the criminal act to be intermittently caused by AI use, though AI acts as a contributing factor but not an enforcing, investigating or a moderating factor toward crime (King *et al*., 2018). A criminal offence can be liable to an individual or a corporation provided the component of criminal act and the mental component consisting of the general or the know—how in relation to the conduct of the criminal act has to be proven. Once it is proved that the act was with a criminal intention, the entity is liable for a prosecution for the offence (Macdonald, 2015). The matter of concern is whether AI systems could qualify the two requirements needed to be claimed as a criminal liability. There are a number of opposing opinions stating that the inappropriateness of criminal law to be held as a mechanism to hold an AI agent accountable (Lima, 2017). It was contended that mental component is related to human agents with a criminal intension including criminal liability. There is, however, nothing more to be considered than as group of entities made of human serving as agents together. The criminal liability as per law is defined to be a liability owed by human or human representing a corporation, whereas AI is completely unique and autonomous.

AI still lacks to be equivalent in capacity for emotional and intellectual abilities as humans. However, in the near future, it may be considered to be at par. The scenario in that era, when this becomes a reality, could be with huge difference in relation to criminal law and its eligibilities to AI agents. By then, humanity would consider AI agents equally capable of being sued for a criminal liability and for being engaged in malicious acts. This will also invite AI to be a part of the judicial and legislative processes.

5. RESPONSES TO ARTIFICIAL INTELLIGENCE CYBERCRIME INTIMIDATIONS

AI as a term discusses a ray of hope to users, but AI fears to mankind are again not new but a couple of things need to be considered (Calo, 2017). One is the increasing strength in the ability to computing and the access to training data has produced a dramatic revolution in machine learning, which further harvests huge AI potential having both pros and cons. On the other hand, the grabbing of attention of the policy makers toward AI, precisely toward cybercrime fears.

Considering the gradual developments with AI, specifically related to the management of stress between the pros of AI and the threats that occur due to the probable risk imposed by AI systems, there are a lot of arguments and concerns highlighted with respect to the regulations, statutory requirements and legal governance of AI, data technologies, robotics, and machine learning autonomy. It was highlighted by a former FBI deputy director stating that the cybercrime works faster, it happens at coding speed, at network speed, while the legal prosecution agencies have a human speed of execution comparatively to deal with the criminal act (Knowledge Wharton, 2018). This indicates that the private and public sector entities need to have serious interventions with resources and with various collaborations to investigate and resolve the threats in an efficient way. In case of the USA, majority of such interventions are done by the private sectors, as 98% of the relevant infrastructure and required tools were and are still owned by the private sector of the country (Knowledge Wharton, 2018). As human increases its dependency on machine learning, AI will conduct multiple tasks on his behalf. The global legal systems need to address such plan of actions that in case of damages caused by AI systems, it would support and decrease such harm. This Indicates an alarm to all economies

around the globe to observe the pros and shortcomings of AI regulations at the earliest (Scherer, 2015). Many institutions including the United Nations are working on to develop favoring procedures to safeguard and ensure that AI including other technology would be supportive and not harmful to mankind (Muggah and Kavanagh, 2018).

6. CONCLUSION

Financial crimes or economic crimes in general refer to such criminal acts which are nonviolent in nature but they result in financial losses to the victims (IMF, 2001). It is also termed as any illegal action performed by an individual entity or groups of individuals, where the indication is to acquire a professional or financial gain from a perpetrator's perspective. Cybercrime is a highly influential terminology, holding a huge population as victims. Millions of people globally are victimized with theft of their personal information or compromised. One of the main reasons for growth in cybercrime may be attributed to a speedy adoption of latest technology undertaken by the cybercriminals.

Financial services are the biggest targets for cybercriminals. Organizing AI solutions would be supportive to AI systems deployed to defend government and business systems from cyberattacks (Yeoh, 2019). However, the concern over the criminal liability of the AI entities has always been a question. Criminal law may not sustain to be as an appropriate solution for holding the AI agents accountable for the crimes. Thus, AI systems are still not deemed to be capable of forming a proper legitimate system in order to curb the financial crimes.

AUTHOR CONTRIBUTIONS

All authors contributed equally to this study.

CONFLICT OF INTEREST

None.

REFERENCES

Bentley PJ, Brundage M, Häggström O, Metzinger T. 2018. Should we fear artificial intelligence? In-depth analysis. European Parliament.

Brown SD. 2016. Cryptocurrency and criminality: The Bitcoin opportunity. The Police Journal, 89(4): 327-339.

Bussmann KD. 2007. Economic crime: people, culture and controls. The 4th biennial Global Economic Crime Survey. Investigations and Forensic Services. Pricewaterhouse Coopers.

Calo R. 2017. AI policy: a primer and roadmap, University of California Davis, Vol. 51: pp. 399-435.

Castells M, Cardoso G. 2005. The network society: from knowledge to policy. Washington, DC: Center for Transatlantic Relations, Paul H. Nitze School of Advanced International Studies, Johns Hopkins University.

Craig D. 2018. Why we need to talk about financial crime, World Economic Forum (WEF).

Everette J. 2017. Risks and vulnerabilities of virtual currency. Cryptocurrency as a payment method. Public-Private Analytic Exchange Program.

Forwood P, Bolton P. 2018. Getting real about AI and financial crime, Pricewaterhouse Coopers (PwC).

France-Presse A. 2018. Global cybercrimes costs $600B annually-study, Inquirer February 22, 2018.

Frunza MC. 2016. Cybercrime. M-C Frunza, Introduction to the theories and varieties of modern crime in financial markets. Amsterdam: Elsevier: 207-220.

Furman J, Seamans R. 2018. AI and the economy (No. w24689). Cambridge, MA.

Gottschalk P. 2010. Categories of financial crime. Journal of Financial Crime, 17(4): 441-458.

Hoadley DS, Lucas NJ. 2018. Artificial intelligence and the national security, Congress Research Service (CRS) Report R45178.

IMF. 2001. Financial system abuse, financial crime and money laundering, IMF Background Paper, available at: www.imf.org/external/np/ml/2002/eng/021201.htm.

Jung J, Lee J. 2017. Contemporary financial crime, Journal of Public Administration and Governance, 7(2): 88-97.

King T, Aggarwal N, Taddeo M, Floridi L. 2018. Artificial intelligence crime: an interdisciplinary analysis of forseeable threats and solutions, Oxford Internet Institute, University of Oxford Paper.

Knowledge Wharton (KW). 2018. Can anything stop cyber-attacks?, KW19 July, Available from: www.knowledge.wharton.upenn.edu/article/creating-tougher-defenses-cyber-attacks.

Lavion D, Rivera K, Elliott S. 2018. Pulling fraud out of the shadows: global economic crime and fraud survey. PwC Global Economic Crime and Fraud Survey Report, Available from: https://pwc. com/.../global-economic-crime-and-fraud-survey-2018-summary-inf.

Lewis J. 2018. Economic impact of cybercrime—no slowing down, CSIS Report February, Available from: www.csis.org/analysis/economic-impact-cybercrime.

Lima D. 2017. Could AI agents be held criminally liable: artificial intelligence and the challenges for criminal law. SCL Review, 69: 677.

McGuire M. 2012. Technology, crime, and justice: the question concerning technomia. Routledge.

Macdonald S. 2015. Text, cases and materials on criminal law. Harlow: Pearson Education Limited.

Macaulay T. 2017. Cybercrime and financial crime: different sides of the same coin, Available from: www.sector.ca/.../disconnect-between–suites-leaders-and-it-teams-in-defending-agai.

Muggah R, Kavanagh C. 2018. 6 ways to ensure AI and new tech works for—not against humanity, World Economic Forum (WEF), July 5, Available from: www.weforum.org/.../2018/07/unitednations-artificial-intelligence-social-good.

Pickett KS, Pickett JM. 2002. Financial crime investigation and control. New York, NY: John Wiley and Sons.

Ryder N. 2011. Financial crime in the 21st century: law and policy. Edward Elgar Publishing.

Ryder N, Turksen U, Hassler S. (Eds.). 2014. Fighting financial crime in the global economic crisis. Routledge.

Scherer MU. 2015. Regulating artificial intelligence systems: risks, challenges, competencies, and strategies. Harvard Journal of Law & Technology, 29: 353.

Treasury Committee. 2018. Oral evidence: economic crime, House of Commons Report HC 940 July 4. UK Cabinet Office 2016, Britain's cyber security bolstered by world-class strategy, UK Cabinet Office Paper 1 November.

United Nations Office on Drugs and Crime (UNODC). 2005. Economic and financial crimes.

Yeoh P. 2019. Artificial intelligence: accelerator or panacea for financial crime? Journal of Financial Crime, 26(2): 634-646. https://doi.org/10.1108/JFC-08-2018-0077