The Impact of the Coronavirus Pandemic on the Commission of White-Collar Crimes by Ordinary Citizens

Eldad Bar Lev
"Alexandru Ioan Cuza" University of Iasi,
Doctoral School of Economics and Business Administration, Romania
eldaddl@bezeqint.net
Liviu-George Maha
"Alexandru Ioan Cuza" University of Iasi,
Faculty of Economics and Business Administration, Romania
mlg@uaic.ro

Abstract

The white-collar frauds have seen an increase in recent years, while the emerging of new digital technologies contributed to an increase of the financial frauds, especially during the global financial crisis of 2008 and in time of coronavirus (Covid-19) pandemic. This article reviews the white-collar scams that gained momentum during the coronavirus pandemic and examines why ordinary people turned into 'white-collar criminals' during this period. The main finding is that the pandemic crisis led to an economic crisis, while people was more focused on committed financial frauds in order to guarantee the economic welfare of their families or the business' survival.

Key words: scams, financial fraud, white-collar criminality, Ponzi schemes
J.E.L. classification: D91, E26, K42

1. Introduction

A time of economic uncertainty due to the global pandemic creates opportunities for 'white-collar' criminals to increase their practices. In the United States, the largest economic frauds were committed during the financial crisis (Iacurci, 2020, p. 1).

The Covid-19 pandemic has beset societies around the world with very complex public health, social and economic crises. In time of such economic instability, the number of frauds increases. Even before the corona pandemic, financial fraud was a business that rolled in $5 trillion a year. The situation that arose, along with the helplessness and economic uncertainty, prompted many law-abiding citizens to commit tax, financial and cyber offenses. The dwindling living standards, shortage of basic products, and collapse of many small businesses due to the lockdown prompted such citizens to commit, willingly and unwillingly, scams that would allow them to survive and to increase their income through illegal ways (Doron & Peretz, 2021). 'Corona Coins' scam is an example of a specific effective fraud that has arisen recently, based on the mania of crypto currency investors. Due to the corona pandemic, cryptocurrencies will be rarer and more expensive as more people are affected by the pandemic.

The paper aims to review the white-collar frauds that increased during the coronavirus pandemic and to examine factors and motives of why ordinary people turned into 'white-collar criminals' during this period. This paper is structured as follows. The second section presents the theoretical background regarding white-collar crime, while the third one provides the research methodology. The next section shows an analysis of the economic frauds before the pandemic and of what happened during the Covid-19 crisis. Finally, the conclusions are presented.

2. Theoretical background

'White-collar delinquency' was first defined by Edwin Sutherland (1949), who described a white-collar offender as a respected figure with high-status in his community, who commits an offense relating to his occupation. This definition of Sutherland has two main critics. On the one hand, Sutherland was a sociologist and criminologist, but not a legal expert. Hence, his definition may be influenced by social rules and the social surroundings. He examined the effects of the social surroundings, while jurists are more interested in the aspects defined by the law. On the other hand, Sutherland refers primarily to the social status of the suspect, while white-collar offenses are not defined solely by the social status of the offender. Even today, there is no consensus on the definition of 'white-collar' crimes in terms of criminal law.

A more in-depth analysis as to the definition of white-collar crime is found at Kenneth Mann (1992), who addressed distinguishing characteristics of white-collar crimes. He determined that not only the upper stratum, but also members of the middle class commits white-collar frauds. After examining the nature of the characteristics, Mann defined the term 'white-collar crime' as the exploitation of special resources (job, assets and political influences) to generate illegal profits through camouflage and deceptive methods, and the prevention of discovery of the act by exercising control over resources of information. The legal definitions of criminal prohibitions create a marked ambiguity between what is considered a felony act and one that merely creates civil liability.

Mann's definition highlights two important points regarding assessment of the magnitude of the white-collar crime and the application of sanctions against it. Firstly, the phenomenon is broader than we tend to think. It is difficult to reveal information about the commission of such offenses, with only the tip of the iceberg appearing on the surface. This finding suggests that the economic damage resulting from white-collar offenses is enormous and severely impairs society's ability to advance its goals. Secondly, the definition emphasizes the need for effective means of inquiry. The more complex the camouflage methods that are employed within organizations or companies that possess highly sophisticated means, the greater the expertise that is required on the part of investigators to disclose them (Mann, 1992).

3. Research methodology

The methodology used to conduct this paper includes a black letter research method. This method implies an analysis of primary and secondary data by using reports and newspapers on several types of white-collar crimes. The research method provides an analysis of several typologies and cases regarding white-collar crimes in order to provide a double perspective about these fraudulent schemes. On the one hand, the method used helps to frame the theoretical background of the research and the manner in which these fraudulent acts happen in practice. On the other hand, various relevant case studies and examples from different countries were presented to prove several typologies and trends of white-collar crimes during the crises.

4. Findings

4.1. The situation before the Covid-19 pandemic

Significant changes in crime were found relative to the trends that preceded the outbreak of the Covid-19 pandemic during the lockdown period, starting with March 2020. Crime in the pre-Covid-19 period in Israel was about 20% higher than during the pandemic, with 9,503 cases opened in 2019 compared to 7,576 opened in the Covid-19 period (Summerfield, 2022).

In the field of white-collar fraud, there has actually been a significant reversal of the trend. Before the Covid-19 period, these offenses were much less common. Offenses of phishing, fictitious emails and fictitious loans gained significant momentum due to the many lockdowns that were imposed on the public (Summerfield, 2022).

Most of the white-collar frauds were committed during the financial crisis of 2008 all around the world. In South Africa, the Reserve Bank reported that thousands of persons lost out to illegal investment schemes or deposit-taking arrangements every year. More than 200 schemes were

investigated between 2007 and 2011, while victims included pensioners and recipients of government benefits (Summerfield, 2022). China has become a pillow for such huge financial frauds that the authorities have defined the phenomenon as a real threat to social order. Two common versions in China of Ponzi scams: one in which investors are recruited through the promise of a quick profit without risk provided they recruit additional investors and the other in which young people are taken captive and forced to recruit investors. This version is causing a stir on social media in China due to several suicides that have occurred within its framework. The Chinese authorities have taken steps to eradicate this phenomenon. One of the reasons for the blossoming of the frauds is loose regulation on financial entities operating in the network, alongside greed and a desire to get rich that have become a major driving force among Chinese society.

In the United States, the largest frauds occur during the financial crisis. For example, Rothstein & Rosenfeldt was a law firm founded by Scott Rothstein and Stuart Rosenfeldt, but the first used it to fraud people by selling discounted stakes in fraudulent settlements and lawsuits. Between 2005 and 2009, Rothstein convinced investors that the scheme was real by fake settlement papers, bank statements, personal guarantees and false court order. Rothstein used the money from the scheme ($1.2 billion) to finance his company, buy equipment, pay employees and rent for offices, but also to gain political influence, buy properties, cars and live a generous lifestyle. When the scheme started to fail, he was sentenced to 50 years in prison, while his former law partner denies any involvement in the scheme (Bloomberg, 2011).

Another example is Gabriel and Marco Bitran, who founded GMB Capital Management in 2005 in order to manage hedge funds. They promised to investors huge returns ranging from 16% to 23%, with no decrease over the years, by using a complex trading model developed by Gabriel Bitran based on his research at Massachusetts Institute of Technology. In the fall of 2008, several of the hedge funds had disastrous losses, resulting in investors losing 50-75% of their principal in many instances. Both paid $4.8 million fine and were denied a license to engage in future investments (SEC, 2012).

In Israel, a similar example is Eran Mizrahi who deceived people by presenting false documents and financial statements, promising high returns for their funds. In the period 2007-2012, he used its company to attract funds amounting to 57 million shekels, while the investors' money was used in personal purposes. In 2012, the authorities caught him and he received 12 years in prison (Levi, 2016).

As it can be seen from these examples, white-collar offenses include economic offenses such as tax evasion, money laundering, VAT offenses, Ponzi scams and more. Punishment in Israel for these offenses has changed greatly over the years. In the past, offenders received moderate punishment, and cases would usually be terminated with fines and service work being imposed on the perpetrators. Today, that has changed so that more severe punishment is dispensed, including long prison sentences. In 2004, a man with no criminal record was convicted for tax evasion of about nearly 5 million shekels and was sentenced to service work alone. In contrast, in a relatively similar case, from 2016 a man with no criminal record was convicted for tax evasion of about nearly 10 million shekels and was sentenced by the court to ten years in prison. Well-known are the cases that recently ended in long prison sentences for prominent figures in the Israeli economy (Abohav, 2020).

During the covid-19 pandemic, however, punishment for white-collar crimes backslid to the same as in 2004. Judges demonstrated 'understanding' towards ordinary people who were caught committing such offenses. The difficult economic situation had landed on the court's doorstep.

4.2. The situation during the Covid-19 pandemic

The assumption of this article is that law-abiding citizens would not have committed these offenses had they not been in financial distress. Prolonged periods of lockdown led to a change in consumption patterns, and tremendously increased the use of cyber networks during the pandemic. This situation gave rise to cyber-attacks and ransom demands as had happened to many companies, especially the ransomware attack on the servers of the Israeli insurance company Shirbit. Another trend is the hacking of companies' databases or from organizations, alongside with acquisition of items without payments, information theft and phishing (Doron & Peretz, 2021).

In times of crisis, alongside the positive effects of social responsibility and many relief actions intended for victims and society, there is evidence of fraud, which is enhanced by advanced technologies in the fields of communication, finance and the dissemination of information. Another type of fraud that was common during the coronavirus pandemic is phishing, which represents the theft of identities and credit card information. Some people had set up websites posing as legitimate websites or claiming to provide assistance. Two months into the lockdown in the United Kingdom became evident for those seeking to take advantage of the anxiety and uncertainty that the pandemic had created. Therefore, new frauds appeared. For example, industry insiders, especially those in the financial services sector had become acquainted with Covid-related e-commerce scams, which clearly included fake or non-existent hand sanitizer or personal protective equipment. In Israel, there was an increase of about 30% in the number of cyber-attacks during 2020 (Kristal, 2020).

The spike in white-collar crime caused by the pandemic is reflected in enforcement activities instigated by regulatory bodies. For instance, as of late March 2021, the United States Department of Justice has publicly charged 474 defendants with criminal offenses related to Covid-19 fraud schemes. Many of these cases involved efforts to obtain over $ 569 million from the U.S. government and individuals by fraud (Summerfield, 2022).

However, Covid-19 significantly influenced the government's ability to investigate and prosecute white-collar crime. In-person investigations and interviews were curtailed. Agents struggled to develop cooperating witnesses, which typically requires face-to-face meetings to build trust. Though video conferencing technology bridged some of the gaps in communication, it was less likely to be used in highly sensitive plea negotiations, which slowed authorities' ability to move cases forward (Summerfield, 2022).

The fraudulent outline is carried out through several patterns, such as miracle drugs, home tests and fake vaccines, as well as loans from private entities and, third, contacting victims through different methods.

4.2.1. Miracle drugs, home tests and fake vaccines

One way the crooks of the coronavirus era are taking action is by marketing a variety of counterfeit products on e-commerce sites. At the various sites you can find, for example, fake medicines that guarantee full protection against the virus, homemade Covid-19 tests at unrealistically low prices and mini potions that are supposed to cause a speedy recovery from the serious disease. In order to prevent these situations, before making any purchase online, it is necessary to pay attention to two main warning signs (Misan, 2020):

- The payment method: a legitimate and reliable site will allow the payment through PayPal. On the other hand, a website established with the aim of defrauding and nothing more, will allow the payment only by bank transfer.
- Miracle medicines: it is necessary to understand whether the products offered for purchase on the site are real and legitimate products. If the transaction involves a new drug that no one has yet heard of, then this is a fraud and nothing more.

These warning signs need to be checked really well and preferably several times before swiping the credit card.

4.2.2. Loans from private entities

A significant increase in the scope of fraudulent private sector loans since the beginning of the Covid-19 crisis was recorded. The criminal behavior of offenders in this sector is unparalleled: victims receive a phone call from a friendly and polite representative, who promises them wonders and miracles. One may be promised, for example, a large loan with unusually favorable terms, a loan that will be disbursed to the bank account within a few hours, or a loan does not require signing a contract or having to prove repayment capacity. All these practices are intended to make the proposal particularly attractive and to impair one's judgment. Next, the victim will be asked to transfer a "negligible" amount of money to the accompanying party, on the pretext of him having to pay handling fees prior to opening a loan account and beginning the loan process. Once such payment is transferred, the company's representative will no longer be accessible and no loan money will be

transferred to the victim's account. Countless offenders in Israel spend day and night locating people who need quick access to money and who are willing to risk a few thousand shekels to get a loan as quickly as possible (Misan, 2020).

Nevertheless, it is crucial for anyone who has suspicions to verify the company's legitimacy, to demand a contract and to refrain from paying any handling fees or other payments until there is a certainty that it is a legitimate and recognized company.

Another method currently employed by offenders is to offer extremely low or extremely high prices. Both inflated prices and irrational bargain prices should raise a red flag indicating fraud. In order to encourage victims to transfer payment, the perpetrator may pressure them by telling them, for example, that the attractive opportunity will expire within the next few minutes. In the vast majority of cases, these are tactics designed to apply pressure for the victim to act hastily and without judgment (Misan, 2020).

4.2.3. Other fraudulent methods

One fraudulent method is to contact victims by using email addresses and websites that pose as websites of well-known pharmaceutical companies and medical equipment manufacturers. This kind of fraud is exploiting a market that has a limited supply of masks and medical equipment in the face of huge demand. The victim is asked to transfer payment to a bank account, usually in Germany, the Netherlands, Spain or Portugal, in exchange for the transfer of medical protective equipment. There is also the phenomenon of sending emails on behalf of the so-called World Health Organization, which contain a link to websites that supposedly provide medical advice to the public, recommendations for defensive methods, and other updates such as a global expansion map. By clicking on the link and opening the site, the victim is required to provide identification details, including an email address and password, enabling the offender to implant malware on the cellphone and to steal personal information (Kristal, 2020).

Another method is to contact the elderly population by phone. The caller impersonates a doctor and tells the elderly victim that his or her relative has been hospitalized after having contracted Covid-19 and that there is urgent need to transfer payment so that they can receive life-saving care. Payment is made either through a money transfer or by arriving at the victim's home and collecting it in person. A fraud of the same type had been realized in Israel in the past nicknamed 'The Lithuanian Sting'.

Another outline is impersonating representative of a medical institution and contacting the victim, under the pretense that he may have been exposed to the virus and that the call is intended to trace the chain of infection. As part of the supposed verification process, the victim is asked to disclose the personal information, including bank account details (Kristal, 2020).

A 2019 study in Norway found that over a period of one year, people commit property crimes by 60% more after losing their jobs, including theft from a private person as well as burglary and destruction of property. These figures relate to Norway, where the employment rate and per capita income are relatively high, and the crime rate is low (Benjamin, 2020).

Therefore, the hypothesis is that in various countries, including in the United States, where job losses can have a serious impact on the economic situation, there is an expectation for an increase in the level of crime. This fact is mainly due to the need to supplement income, but also out of the need for unemployed people to protect against mental distress (Rege et al., 2019).

The Association of Certified Fraud Examiners (ACFE) is the world's largest organization engaged in training and training professionals to deal with the prevention of fraud and embezzlement and the fight against corruption and fraud in organizations. In December 2020, ACFE has published a report following a survey on the impact of the covid-19 pandemic in the fight against embezzlement and fraud. The main findings of the report are that 79% of respondents had already experienced or anticipated an increase in the overall level of fraud, while 38% of them noting that this increase was significant. The outlook for 2021 was that 90% of respondents have expected a further increase in the overall level of fraud over the next 12 months, while 44% of them said that the change would likely be significant. Cyber fraud (such as hacking, ransomware and malware) is the highest risk, with 85% of respondents already seeing an increase in fraud, and 88% expecting another increase

over the next years. Other significant fraud risks observed for 2021 are identity theft and payment fraud, such as credit card fraud and fraudulent mobile payments (Assaf, 2021).

5. Conclusions

The main finding of this paper is that the number of frauds and the one of fraudsters increase in time of each economic uncertainty. The Covid-19 pandemic has led to an economic and social crisis, which has brought ordinary people to commit economic crimes. These offenses are not necessarily committed with the intention of getting rich, notwithstanding that they may be among the more serious economic offenses. Rather, the aim of these economic frauds is to prevent the economic collapse of the fraudsters' families or businesses. Remains questionable if the harsh punishment that the justice system seeks to apply is justified in these situations for ordinary persons. After all, law enforcement systems did not anticipate such a situation.

The justice system will have to be flexible and carefully examine cases in which the Covid-19 crisis constitutes mitigating circumstance relating to the offenses committed. It will have to lessen the severity of punishment again, considering that for an ordinary person, severe punishment that includes imprisonment is comparable to a death sentence. In addition, the justice system must think to the plight of the persons that may be entangled in these offenses and take into account that the government does not provide the necessary economic response to aid the population.

The price increases, the rise in interest rates and the spike in the cost of living are expected to stimulate the frauds that arose during the pandemic. The risk of fraud occurring in all sectors requires all businesses to ensure that they have procedures in place to mitigate these fraud possibilities, so that they remain fully protected.

Regarding the population own protection, each person must be well informed and to think twice before disclosing credit card information, entering the ID number on a website, transferring even a small amount of money, or signing a contract with any party. Before any decision, especially when having doubts, each person must consult at least one person that truly trust.

References

- Abohav, E., 2020. The corona crisis will change the penalty pendulum in white-collar offenses, *Calcalist*, 26 April, [online]. Available at https://www.calcalist.co.il/local/articles/0,7340,L-3811473,00.html. [Accessed 17 June 2022].
- Assaf, N., 2021. Corona crisis: how to prepare for the expected increase in cases of embezzlement and fraud. *Israel Institute of Internal Auditors*, [Hebrew], Issue 14: Brightness in Days of Surplus, September, [online]. Available at https://theiia.org.il/articles/. [Accessed 15 June 2022].
- Benjamin, L., 2020. Effects of the corona plague and distance policy on crime: comparative review, *Ministry of Internal Security*, [Hebrew], March 30, [online]. Available at https://www.gov.il/BlobFolder/reports/corona-effect-on-crime-ii/he/publications_batap_olami_corona-effect-on-crime-2.pdf. [Accessed 15 June 2022].
- Bloomberg, 2011. Rothstein gets 50 years in prison for $1.2B Ponzi, *Bloomberg,* December 23, [online]. Available at https://www.investmentnews.com/rothstein-gets-50-years-in-prison-for-1-2b-ponzi-29577. [Accessed 20 June 2022].
- Doron, E. and Peretz, S., 2021. When law-abiding citizens become tax offenders, *Finance* [Hebrew], 24 March, [online]. Available at https://finance.walla.co.il/item/3425511. [Accessed 20 June 2022].
- Iacurci, G., 2020. Ponzi schemes hit highest level in a decade, hinting next 'investor massacre' may be near, *CNBC*, February 11, [online]. Available at https://www.cnbc.com/2020/02/11/ponzi-schemes-hit-the-highest-level-in-10-years.html [Accessed 15 June 2022].
- Kristal, Z., 2020. Cyber fraud against the background of the Covid-19 pandemic, Posta [Hebrew], [online]. Available at https://posta.co.il/article/78696786-2/. [Accessed 20 June 2022].
- Levy, Z.S., 2016. The Supreme Court rejected the appeal of Eran Mizrahi, who was sentenced to 12 years in prison for a huge scam, *Calcalist* [Hebrew], March 17 [online]. Available at https://www.calcalist.co.il/local/articles/0,7340,L-3683850,00.html. [Accessed 15 June 2022].
- Mann, K., 1992. White-collar crime and the poverty of the criminal law. *Law & Social Inquiry*, 17(3), pp. 561-571.
- Misan 2020. Good to know *Magazine* [Hebrew], article's date December 2020, [online]. Available at. https://www.mishan.co.il/good_to_know [Accessed 17 June 2022].

- Rege, M., Skardhamar, T., Telle, K., and Votruba, M., 2019. Job displacement and crime: Evidence from Norwegian register data. *Labour Economics*, 61, 101761.
- SEC, 2012. SEC charges father-and-son hedge fund managers who agree to pay $4.8 million to settle fraud case. *U.S. Securities and Exchange Commission*, April 20, [online]. Available at https://www.sec.gov/news/press-release/2012-2012-71htm. [Accessed 20 June 2022].
- Summerfield, R., 2022. White-collar crime in the post-COVID-19 landscape, *Financier Worldwide Magazine*, February, [online]. Available at https://www.financierworldwide.com/white-collar-crime-in-the-post-covid-19-landscape#.YsvoDHZByUl. [Accessed 15 June 2022].
- Sutherland, E. H., 1949. *White-collar crime*. New York: Dryden Press.