The impact of the coronavirus pandemic on the commission of white-collar crimes by ordinary citizens

Eldad Bar Lev

Abstract

The COVID-19 period has led us to a political economic crisis, which has brought normative people to commit economic crimes - not with the aim of getting rich or making easy money, but with the aim of preventing the economic collapse of their family or business. These offenses are not necessarily committed with the intention of getting rich, notwithstanding that they may be among the more serious economic offenses. This article reviews the white-collar scams that gained momentum during the coronavirus (COVID-19) pandemic and examines why normative people turned into "white-collar criminals" during the COVID-19 pandemic that broke out in December 2019. Why and how did this happen? and also reviews the situation before the pandemic, during the pandemic and after it.

Keywords: Scams, financial fraud, white-collar criminality

Introduction

Definition - what is white-collar delinquency?

"White-collar delinquency" was first defined by Edwin Sutherland (1949) [11], who characterized/identified/described a white-collar offender as a respected figure with high-status in his community, who commits an offense relating to his occupation. (Sutherland, 1949) [11].

This definition of Sutherland has two main critics

A. 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.

B. 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. It should be noted that 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 in the writings of Kenneth Mann (1992) [9], who addressed distinguishing characteristics of white-collar crimes and determined that white-collar offenses are committed not only by the upper stratum, but also by members of the middle class. After examining the nature of the characteristics, Mann defined the term "white-collar crime" as follows: The term "white-collar crime" refers to 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, while 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, 1992) [9]. This definition highlights two important points regarding assessment of the magnitude of the phenomenon of 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) [9].

The COVID-19 pandemic has beset societies around the world with very complex public health, social and economic crises. 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, 2020) [8].

2. 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. The first, March 2020

According to data from Israel, 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.

The most significant decline in the number of cases/crimes occurring during the pandemic was recorded in apartment break-ins – the decline of 45% and in break-ins to businesses and institutions -showing a reduction of 7% in criminal incidences. In the field of white-collar media 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.

White-collar offenses include economic offenses such as tax evasion, money laundering, VAT offenses, receiving anything fraudulently 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. (Abbohav, 2020) [10].

For comparison, one can see the difference between the punishments imposed in similar cases (17277: one can see how the severity of punishments evolved over the years):In 2004, a man with no criminal record was convicted for tax evasion in the amount of about nearly NIS 5 million, 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 in the amount of about nearly ??? NIS 10 million, 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. (Abbohav, 2020) [10].

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

3. 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”), hacking into databases of companies and organizations and information theft, phishing - theft of identities and credit card information, acquisition of items without payments, etc. (Doron, 2020) [5].

According to data from the National Cyber Network, during 2020 there was an increase of about 30% in the number of cyber-attacks in Israel. Thus, this study examines the link between financial stress during the COVID-19 pandemic and the inclination of normative law-abiding? Citizens to commit financial crimes. (Krisel, 2020) [3].

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. (Krisel, 2020) [3].

Two months into the lockdown in the UK it became???? Evident that new scams were being perpetrated by those seeking to take advantage of the anxiety and uncertainty that the pandemic had created. 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. (Krisel, 2020) [3].

Another type of fraud that was common during the coronavirus pandemic is phishing. Some people had set up websites posing as legitimate websites or claiming to provide assistance. The Rogue sought unsuspecting citizens who entered personal information on these sites, such as “name, surname, date of birth, ID number and bank account number to which the aid money was supposed to be transferred, with the malicious intent of committing identity or data theft.. (Krisel, 2020) [3].

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 (DOJ) has publicly charged 474 defendants with criminal offenses related to COVID-19 fraud schemes. Many of these cases involved efforts to obtain over USD 569m from the US government and ‘unsuspecting individuals’ through fraud. (Summerfield, 2022) [4].

But COVID-19 significantly impacted the government’s ability to investigate and prosecute white-collar crime. In-person investigations and interviews were curtailed. Agents struggled to develop /engage 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) [4].

~ 19 ~
The fraudulent outline is carried out through several patterns

A. 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. Please note – before you make any purchase online, Need to check really well and preferably several times and make sure to think twice before swiping your credit card. Pay particular attention to the following warning signs:

The payment method – a legitimate and reliable site will allow you to pay through PayPal. On the other hand, a website established with the aim of defrauding you and nothing more, will allow you to pay by bank transfer only.

Miracle Medicines – try to understand whether the products offered for purchase on the site are real and legitimate products. If you have been offered to purchase a new drug that no one has yet heard of, rest assured that this is a scam and nothing more. (Misan, 2020) [8].

B. Loans from private entities
We can also see a significant increase in the scope of fraudulent private sector loans since the beginning of the COVID-19 crisis. The criminal behavior of offenders in this sector is unparalleled: victims receive a phone call from a friendly and polite representative, who promises those 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 of the above ploys are intended to make the proposal particularly attractive and to impair one's judgment. (Misan, 2020) [8].

Next, the victim will be asked to transfer a "negligible" amount of several hundred or thousand NIS 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.

It is important to understand that the field of nonbank loans is a particularly dangerous area. There are countless offenders in Israel who spend day and night locating people who need quick access to money and who are willing to risk a few thousand NIS to get a loan as quickly as possible. Even in this case, nevertheless, it is crucial to rummage through the tassels of the company that offers you the credit, verify its legitimacy, demand a contract and study it thoroughly, and refrain from paying any handling fees or other payment until you are certain that it is a legitimate and recognized company.

The cost – 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 (Misan, 2020) [8].

Attempt to apply pressure – 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 for the victim to act hastily and without judgment, therefore, it is important to avoid succumbing to pressure and making any rash decisions. (Misan, 2020) [8].

C. Other fraudulent methods
Contacting 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 exploits a market that Hasa 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. (Kristal, 2020) [3].

Another variation: contacting 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 scam of the same type had been perpetrated 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 relinquish personal information, including bank account details.

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 steal personal information. (Kristal, 2020) [3].

A 2019 study in Norway found that unemployment people commit property crimes, over a period of one year, by 60% more after losing their jobs, including theft from a private person as well as camps, burglary and destruction of property. Those who committed the crimes have 20% more police cases at a time when they were not working. The researchers emphasize that these figures relate to Norway, where the employment rate and per capita income are relatively high, and the crime rate is low. (Gov, 2020) [6].

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, you can expect a more extreme response of participation. In crime, mainly due to the need to supplement income, but also out of the need to protect against mental distress. (Rege, 2020) [2].

In December 2020, the ACFE (Acfe of Certified Fraud Examiners), 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, published a report in December 2020 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 presented below. (Asaf, 2020) [7]. 79% of respondents in the survey responded that they had already experienced or anticipated an increase in the overall level of fraud, with 38% noting that this increase was significant. Towards 2021, this trend was observed, according to which 90% expect a further increase in the overall level of fraud over the next 12 months, with 44% saying that the change would likely be significant. Cyber fraud (such as hacking, ransomware, and malware) is the highest risk, with 85 per cent of respondents already seeing an increase in fraud, and 88 per cent expecting another increase over the next years. Other significant fraud risks observed and expected towards 2021 are: payment fraud (such as credit card fraud and fraudulent mobile payments), identity theft, and more. (Asaf, 2020) [7].

4. Conclusions
The COVID-19 period has led us to a political economic crisis, which has brought normative people to commit economic crimes - not with the aim of getting rich or making easy money, but with the aim of preventing the economic collapse of their family or business. These offenses are not necessarily committed with the intention of getting rich, notwithstanding that they may be among the more serious economic offenses. Would the harsh punishment that the justice system seeks to promote be justified in situations where the normative person tries to raise his head above water? After all, law enforcement systems did not anticipate such a situation.

The harsh reality in which we live, the price increases, the rise in interest rates and the spike in the cost of living are expected to exacerbate the scams 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 risks, so that they remain fully protected.

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, as, for a normative person, severe punishment that includes imprisonment - is comparable to a death sentence. In addition, the justice system must remember the plight of the public that may be entangled in these offenses, and take into account that the government does not provide the necessary economic response to aid the public, as reflected in the complicated and complex criteria requirements for granting the public assistance.

Next time, before disclosing credit card information, entering your ID number on a website, transferring even a small amount of money, or signing a contract with any party, think long and hard. Ask yourself if you are making a prudent and calculated decision or if you have any doubts. In case you are still uncertain, you'd do well to consult at least one person that you truly trust.

References
5. Doron E. Tax offenses are common during corona days - Voila! Money (walla.co.il), 2020.