United Nations CTOC/COP/WG.2/2024/3

Conference of the Parties to the United Nations Convention against Transnational Organized Crime

Distr.: General
25 March 2024

Original: English

Working Group of Government Experts on Technical Assistance
Vienna, 3 and 4 June 2024
Item 3 of the provisional agenda*
Organized fraud

Organized fraud

Background paper prepared by the Secretariat

I. Introduction

1. The present background paper was prepared by the secretariat to facilitate the discussion under the agenda item 3 of the provisional agenda of the fifteenth meeting of the Working Group of Government Experts on Technical Assistance. It provides a brief, non-comprehensive overview of the different categories of organized fraud that are used to target individuals or institutions for purposes of obtaining a financial or other material benefit and is aimed at promoting more effective responses to organized fraud within the framework of the United Nations Convention against Transnational Organized Crime.

2. Fraud has evolved significantly over the years, adapting to technological advancements and changes in society. It has become increasingly sophisticated, using psychological manipulation and technology, making use of machine learning, artificial intelligence and other technologies to automate offending. The high volume and severity of fraud poses a significant risk to people, economies and prosperity worldwide, and negatively impacts the public's confidence in the rule of law. However, developing an accurate understanding of fraud presents several challenges. Victims often underreport fraud due to feelings of shame, self-blame or embarrassment, as well as a lack of recognition that a crime has occurred. Moreover, a significant portion of fraud targets businesses, many of which choose not to report these crimes to avoid damaging their reputation. The anonymity and remoteness associated with fraud perpetration further obscure the identity of offenders from both victims and authorities, hindering efforts to assess underlying patterns and associated risks. Furthermore, the dynamic nature of fraud, which is constantly adapting to changes in legal, social, commercial and technological systems, means that new and innovative methods of offence may go unnoticed within static official data.

3. The international community has recognized the worrying scale of fraud and the need for joint efforts in preventing and combating fraud.[1] The General Assembly, in

* CTOC/COP/WG.2/2024/1.

[1] See Economic and Social Council resolutions 2004/26, 2007/20, 2009/22, 2011/35 and 2013/39 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

its resolution 78/229, reaffirmed the mandate of the United Nations Office on Drugs and Crime (UNODC) to, upon request, provide technical cooperation and assistance to Member States in respect of all forms of organized crime, including fraud. This aligns with the purpose of the Organized Crime Convention, which is aimed at promoting cooperation to prevent and combat transnational organized crime more effectively, as articulated in its article 1. Understanding the changing nature of fraud and the increasing use of technology to broaden its reach, the General Assembly, in its resolution 74/177, called upon Member States to explore measures and develop possible conclusions and recommendations designed to create a secure and resilient cyberenvironment, paying particular attention to identity fraud-related offences.

4. It is widely acknowledged that fraud can be an organized and serious crime.[2] The evolution of technology alongside the swift expansion in the scope and magnitude of organized crime has driven the creation of a range of new ways to defraud individuals, businesses and even governments on a massive and global scale. This has empowered organized criminal groups to more effectively target victims around the globe.[3]

5. Fraud within the realm of organized crime possesses distinct characteristics. First, it is primarily concerned with monetary theft rather than the production or distribution of illegal goods, distinguishing it from other criminal activities. Second, many fraudulent activities are carried out remotely, facilitated by technology that enables anonymous communication and the transfer of stolen funds without physical interaction between the perpetrator and the victim. Third, fraud often relies on victims to willingly provide access to their funds, with success hinging on deceitful tactics that blur the line between legitimate and illegitimate entities. These elements shape the methods employed by fraudsters, dictate the necessary capabilities and influence the structure of the organized criminal groups.

6. Some of these fraudsters are embedded within seemingly legitimate businesses or professions. Utilizing insights or skills acquired from operating within ambiguous or unregulated areas outside conventional business or commercial norms, certain organized criminal groups adopt structures reminiscent of legitimate workplaces. This may involve establishing a salaried workforce and implementing a well-defined division of labour, effectively mimicking the organizational frameworks found in lawful enterprises. There is no typical organized criminal group engaged in fraud. Fraud may be committed by a variety of groups, including cybercriminal networks that anonymously trade in technologies, data and other criminal services; organized criminal groups that coalesce around a locality or social networks; organized criminal groups structured to mimic a legitimate workforce (e.g. call centres); and white-collar criminals who commit fraud from within otherwise legitimate organizations or occupations. Instead of hierarchies, organized criminal groups often feature fluid collaboration among their members.

7. However, it is less in the way in which the offenders are organized, but rather the way in which the fraudulent activities are orchestrated that might produce the greater insight into organized fraud. Historically, fraud has not been afforded the same levels of priority given to other types of organized crime, with organized fraud often perceived as a supplementary criminal activity of organized criminal groups involved in other, more serious crimes (e.g. drug trafficking).[4] In the Organized Crime Convention, serious crime is defined as an offence subject to a penalty of at least four years of imprisonment. In practice, however, many States do not criminalize fraud as a serious crime. As a result, it falls outside the scope of the Organized Crime

[2] European Union Agency for Law Enforcement Cooperation (Europol), *Internet Organized Crime Threat Assessment (IOCTA) 2023* (Luxembourg, Publications Office of the European Union, 2023); and International Criminal Police Organization (INTERPOL), "2022 INTERPOL global crime trend summary report" (October 2022).

[3] INTERPOL, "INTERPOL financial fraud assessment: a global threat boosted by technology", 11 March 2024.

[4] Michael Levi, "Organized fraud" in *The Oxford Handbook of Organized Crime*, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014).

Convention. Moreover, even in instances where fraud is punishable as serious crime, sentencing does not necessarily reflect this seriousness.

II. Categories of organized fraud

8. Fraud is a crime that encompasses highly diverse actions and behaviours that are undertaken across a wide range of settings and against diverse victims. In academic research, fraud has been broadly defined as "obtaining something of value or avoiding an obligation by means of deception".[5] Therefore, unlike other forms of serious acquisitive crime, fraud is perpetrated by deception instead of force or coercion. Moreover, the victim and offender are seldom required to be in the same place at the same time, and many frauds cross national and international borders. Fraud features in the criminal laws of many countries, though it is described in different ways and to varying degrees of specificity.[6] Some laws provide a generalized description of the behaviours that constitute fraud, whereas others make reference to certain activities, products or services that are prominent in fraudulent schemes, such as impersonating an authority or the manipulation or unauthorized use of data. Some States have introduced separate legislation to address different facets of fraud offending, for example, computer fraud, credit fraud, auction fraud or fraud against businesses. However, there are some core elements of fraud that feature in most legal definitions: the use of deception to gain an unjust advantage or benefit, causing a detriment to another person or organization. Deception is usually understood as dishonesty, false representations, trickery, artifice, fraudulent manoeuvres, abuse of trust or the concealment or omission of information. The detriment to another is in many cases implied in the benefit to offenders, but some highlight the detriment to another using terms such as affecting or injuring the financial interests of others, a wrongful loss or being defrauded. The detriment can be to an individual, a company or a State.

9. Fraud offending is highly diverse in the methods employed, the entities targeted and the impact on victims and wider systems. Consequently, a multitude of typologies have been developed to understand the nature of fraud. While there are other typologies of fraud recognized at the national and international levels, the present background paper is focused on fraud that targets individuals or public or private institutions for the purposes of a financial or other material benefit. To illustrate this, the following key categories were identified, which will be explained in further details in the following sections of the background paper: (a) consumer products and services fraud; (b) consumer investment fraud; (c) employment fraud; (d) relationship and trust fraud; (e) fraud involving the impersonation of officials; (f) identity fraud; and (g) fraud against businesses or organizations.

10. Within the key categories, the main forms of deception that relate to the victim's expected benefit or outcome of the fraudulent transaction is highlighted. Although these categories are not the preserve of organized criminal groups, the capacity to offend and cause harm is greatly augmented by their involvement. Each category represents a different technique for manipulating victims, but all categories can be transnational and involve co-offenders engaged in an organized criminal group. Some are perpetrated in high volumes and result in a high aggregate impact, whereas in others, the harm is acutely experienced by smaller groups of victims.

[5] Grace M. Duffield and Peter Grabosky, *The Psychology of Fraud*, Trends and Issues in Crime and Criminal Justice Series, No. 199 (Canberra, Australian Institute of Criminology, 2001).

[6] The legal definitions were examined in 26 countries in 7 different regions: Europe and North America; Latin America and the Caribbean; North Africa and West Asia; sub-Saharan Africa; South-Central Asia; Eastern and South-Eastern Asia; and Australia and New Zealand.

A. Consumer products and services fraud

11. Consumer products and services fraud represents one of the most prevalent types of fraud, with high volumes of members of the public reporting being defrauded, targeted or exposed to communications selling fraudulent products or services. This type of fraud involves the sale of products or services that are either non-existent or significantly different from what is advertised. Typically, fraudsters market in-demand products or offer products and services at a cost below what is available in the legitimate market. Some fraudsters will target their advertisements to groups considered to be most susceptible to a specific scheme. The frauds can involve sellers and items that are entirely fictitious but also companies that misrepresent the goods or services that they supply. There can be challenges in confirming a fraud when the product or service is received but is considered to constitute a misrepresentation. Sometimes fraudsters exploit a victim's lack of financial literacy to sell financial services such as loans, insurance plans or pensions products. These commonly relate to products for which the value lies in the future, and victims are either provided an overly optimistic projection of future performance or the risks are not properly explained. The fraudsters may also fail to disclose charges, commissions or the legal requirements to the victim, which can lead to further losses and penalties.[7]

12. Products and services that have commonly been featured in consumer products and services fraud include gemstones, pets, event tickets, medical products, lotteries or prize draws promising big rewards, or financial products and services such as insurance. However, there is a near endless variety of products and services that can be used in fraudulent schemes, as fraudsters seek to continuously adapt and capitalize on new markets and consumer demands.

13. A variety of media are used to market the products and services, including online. These include fake websites, legitimate shopping and auction sites, spam email, post or so-called "boiler rooms" that make high volumes of marketing and sale calls. Some offenders take advantage of a vibrant market in leads lists that are compiled by legitimate or illegitimate means (such as a data breach or online phishing campaign) or even directories of individuals who have fallen victim in the past (so-called "suckers" lists). Information and communication technologies have greatly augmented the capacity to market and sell products and services on a global scale and at comparatively low cost. In some cases, the individual consumer may lose money but depending on the circumstances and methods employed by offenders, a sales platform or financial service provider may incur the financial loss. Key methodologies include:

(a) Fake websites developed for the purpose of marketing and/or selling products and services. The offenders may market the website using digital channels, such as social media or spam email, or they may manipulate Internet search engines to increase the likelihood that those searching for relevant products or services will land on their website;

(b) Fake sellers on legitimate sales, auction or social media platforms who use accounts that are opened with fake or stolen identities. These sellers exploit legitimate platforms that provide access to a large volume of users searching for products and services. For example, one organized criminal group posted hundreds or thousands of listings for high-value items such as automobiles on multiple auction sites.[8]

14. Online consumer fraud need not be sophisticated or complex. The abuse of a legitimate sales or auction site can require little more than a single person to open an account on an auction site and post an advertisement to sell a non-existent product. However, a portion of consumer fraud crimes are transnational and involve organized

[7] See Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (London, The Police Foundation, 2020).

[8] For further information, see United Nations Office on Drugs and Crime (UNODC), Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal, Case law database, *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*. Available at https://sherloc.unodc.org/.

criminal groups. The organization is seldom revealed in the exchange with the victim, but rather in understanding the planning and preparation that sit behind it. The key stages include establishing and marketing the website or platform profile, victim engagement to maintain the deception (or elicit further payment) and the movement of the money. The offenders adopt a variety of methods to receive payments while leaving a limited financial trail. Methods include convincing a payment service provider that their company is legitimate, diverting customers to fake payment sites, asking victims to pay using prepaid debit cards, or the use of third-party accounts of money mules or those opened using stolen or fake identities. Organized criminal groups operating from other jurisdictions commonly enlist co-offenders within the target country to facilitate money-laundering.[9]

B. Investment fraud

15. Investment fraud commonly involves the sale of company shares, bonds or currencies, with some schemes marketing investments into tangible assets that range from property or commercial developments to wines and spirits.

16. The commission of these frauds can require a keen awareness of the contours of regulation and related controls that govern the markets, and the line between legitimate and illegitimate practice can be both permeable and difficult to perceive. In some cases, the offenders exploit trust mechanisms by registering as a regulated entity or exploiting other legitimate actors with regulated status. In occupying this grey margin between legitimate and illegitimate practice, they create barriers to law enforcement or other regulators required to navigate and produce sufficient and robust evidence of deception and demonstrate that a crime has occurred. Indeed, while unethical, some may employ schemes that cause high harm to investors but transpire not to be criminal. Pyramid and Ponzi schemes are a common operating model for offenders, whereby the investment scheme relies on continuously attracting new investors to sustain itself, instead of generating returns from genuine products or investments, which may not even exist.

17. Investment fraud appears to be on the increase, partly due to a rise in fraud that involves cryptocurrency investments. This new medium for investment fraud capitalizes on the speed and agility afforded by digital spaces, permitting offenders to engage in mass-marketing at speed and at relatively low cost.[10] In new financial markets, such as the cryptocurrency market, the challenges in regulation create wider gaps to exploit. The methods that are employed in cryptocurrency investment frauds are variable in both technical complexity and novelty, with some techniques transposed from other methods such as market manipulation and financial grooming, which include the development and marketing of fraudulent cryptocurrency investment platforms and so-called “exit scams” or “rug pulls” that involve artificially inflating the value of scam tokens, which become worthless once the offenders withdraw all the monies invested.

18. The success of investment frauds is contingent on effective communication, using various techniques to persuade prospective investors such as targeted or mass-marketing campaigns; aggressive sales techniques; and the production of resources to establish and maintain credibility and trust, including branding, websites and other marketing materials. Offenders can utilize specific communication channels, or a combination, which are deployed at different stages in the offence. For example, initial contact with a victim may be through a phishing website, which is

[9] Christine Conradt, “Online auction fraud and criminological theories: the Adrian Ghighina case”, vol. 6, No. 1, *International Journal of Cyber Criminology*, (January/June 2012); and Jack M. Whittaker and Mark Button, “Understanding pet scams: a case study of advance fee and non-delivery fraud using victims’ accounts”, *Journal of Criminology*, vol. 53, No. 4 (September 2020).

[10] Arianna Trozze, Toby Davies and Bennett Kleinberg, “Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering”, vol. 46, *Journal of Forensic Science International: Digital Investigation* (2023).

followed by a subsequent sales call by phone, and then continued engagement through a fraudulent website. Fraudsters may use the following methods to engage with the victims:

(a) Telemarketing: the use of call centres or boiler rooms to engage in aggressive marketing and sales, often in the form of unsolicited calls that are targeted using leads lists that are compiled or bought from other legitimate or illegitimate actors who compile and sell this personal information on consumers. In some cases, these lists include individuals known to have previously fallen victim and thus are vulnerable to similar approaches for investment, a problem that is particularly acute for vulnerable elderly victims. Call centres can be managed directly by the offenders running the fraudulent scheme or contracted out to specialists that are able to provide these "boiler room" services. These centres may be located overseas from the victims, sometimes in jurisdictions known to have less robust controls on these activities;[11]

(b) Online: some countries have witnessed a substantial rise in online investment frauds whereby initial contact is made through online communications such as social media, fraudulent websites and applications, which play a key role in the deception. The capacity to engage in large-scale and targeted marketing is greatly enhanced by the accessibility of digital technologies and large datasets on consumers. For example, phishing campaigns can be used to entice and pinpoint individuals with an interest in the product or service that is being offered, providing the basis for targeting subsequent communication. Perpetrators commonly exploit social media and digital communication applications to market their products, in some cases utilizing celebrity or popular culture imagery to persuade victims to invest their money. When these fraudulent cryptocurrency schemes penetrate mainstream financial markets it can lead to staggering levels of financial loss;

(c) In-person: investments often involve large sums of money that are highly significant to victims, and in some cases face-to-face contact remains important to achieving sufficient levels of trust to secure an investment. Some fraudsters target victims from existing social or business connections to exploit a trust that already exists.

19. Investment fraud offenders go to great lengths to cultivate a veneer of legitimacy, and commonly adopt the structures, processes and language of a formal legitimate organization, including a clear division of labour, with a hierarchy and designated roles assigned to personnel. The complexity of the operation is variable, depending on their motivation to avoid suspicion or detection and continue offending.[12] So-called "rip and tear" operations can operate for a short time before disappearing with the investors' money, whereas other schemes can operate undetected for many years.

20. Investment fraud victims experience the highest losses when compared with other frauds targeting individual members of the public.[13] The victims are primed with expectations of a financial return that are entirely false or grossly exaggerated. Many investors lose all or a large portion of their money. Regardless of which specific method is employed, victims are commonly sold an expectation of the value that will be gained from their investment in the future, meaning it can be years after the initial investment before the realization that they have fallen victim. The particularities of the different schemes and underlying deception can be highly variable, but the outcome in such schemes generally involves the investors losing all or a large portion of their money. Some examples include:

(a) A complete deception in which the investment service or product never existed;

[11] Neal Shover, Glenn. S. Coffe and Clintin R. Sanders, "Dialing for dollars: opportunities, justifications, and telemarketing fraud", *Qualitative Sociology*, vol. 27, No. 1 (March 2004).

[12] Michael Levi, "Organized fraud and organizing frauds: unpacking research on networks and organization", *Criminology and Criminal Justice*, vol. 8, No. 4 (December 2008).

[13] See also United States Department of Justice, "Justice Department seizes over $112M in funds linked to cryptocurrency investment schemes", press release, 3 April 2023.

(b) The mis-selling of worthless or overpriced shares for high-risk investments that are unlikely to yield the promised return or may simply fail;

(c) Market manipulation techniques that artificially inflate the value of investments to unsuspecting investors.

21. The significance of the financial loss to victims will depend on their financial or personal circumstances. It may also depend on the methodologies employed by the offenders, such as targeting people's pension savings, which can greatly impact the individual victim,[14] whereas some cryptocurrency investments can be focused to receive smaller amounts but from a greater number of victims. In the case of pyramid and Ponzi scheme victims, those who invest and withdraw money at an earlier stage may not lose any money. Once the money has been stolen, the victim may be re-victimized by the same or other offenders, in some cases purporting an affiliation to a legitimate body. They assert the ability to trace and recover the lost funds but demand an upfront fee from the victim, a scheme known as recovery fraud.

C. Employment fraud

22. Employment fraud involves the mass marketing of fake or misleading employment opportunities on job posting websites. The use of online job advertisements has grown significantly in the legitimate sector, particularly since the global pandemic in which recruiters are offering more flexible working arrangements and home working opportunities. Fraudsters exploit the demand for desirable positions, particularly in those segments of the population where legitimate opportunities of this kind are limited due to insufficient qualifications or training or a lack of available jobs in the local economy.[15] The research indicates it is commonly job-seekers who are the least financially secure or in desperate situations who are targeted by these fraudsters.

23. These frauds commonly entail advertising a job opportunity online that is either entirely fictional or much less profitable than advertised. Examples include advertisements for business opportunities, work from home, or modelling opportunities. In some cases the fraudsters request upfront payments from victims before taking a position; the purported reasons are manifold, including starter kits, travel, training or credit score checks. The result is often that the victim loses money without receiving the promised employment. In other schemes, the fraudsters send counterfeit cheques to victims to pay for the victims' start-up costs before claiming they have made an overpayment and requesting the victim transfers the money back to the offender. The victim loses the transferred money and is left with the cost of the cheque once it is identified as counterfeit.

24. Employment fraudsters can also be motivated to steal personal identity information, which the victims provides during the process of application, leaving them vulnerable to further victimization. And in some cases the job transpires to be criminal in nature. For example, the victim may be drawn into facilitating money-laundering (e.g. as a money mule) or acting as a courier to deliver fraudulently purchased items (i.e. identity fraud). In the most serious cases, the victim becomes subject to trafficking in persons for forced labour and forced criminality.[16]

[14] See Skidmore, *Protecting People's Pensions*.

[15] Alexandrea J. Ravenelle, Erica Janko and Ken Cai Kowalski, "Good jobs, scam jobs: detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic", *New Media and Society*, vol. 24, No. 7 (July 2022), pp. 1591–1610; and Delali Kwasi Dake, "Online recruitment fraud detection: a machine learning-based model for Ghanaian job websites", *International Journal of Computer Applications*, vol. 184, No. 51 (March 2023).

[16] For more information on these two forms of exploitation, see also *Global Report on Trafficking in Persons 2002* (United Nations publications, 2022), as well as UNODC, "Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia: policy report" (Bangkok, 2023).

D. Relationship and trust fraud

25. The processes for establishing trust plays a critical role in any type of fraud. However, in the case of relationship and trust fraud, the offenders foster and exploit the power of personal relationships in developing the trust needed to manipulate and deceive victims, sometimes on multiple occasions. In these frauds the victim does not expect to receive a product or service and instead has the expectation of forming a genuine relationship with the offender. The complexity of these frauds rests less in the exploitation of technical or technological systems and more in the dynamics of the relationship between the victim and perpetrator.

26. Many fraudsters establish relationships online and use social engineering techniques over a period of months or even years to gain the trust of the victim. The victims commonly expect a romantic relationship, but it can take other forms such as a trusted friendship, or even the desire for a relationship with a family member of the victim. A number of studies have identified vulnerabilities within the ageing and elderly demographic related to factors such as loneliness, social isolation and a desire to form new relationships. Criminals target and exploit this vulnerability through a process of befriending or romantic engagement. In addition, offenders may impersonate a family member or friend who is in acute difficulty and in need of money to remedy the situation. Such frauds may be targeted and can incorporate personal details that are taken from social media posts of the friend or relative to make the communication with the victim more credible. This is commonly communicated by text message. There are examples of artificial intelligence used to clone the voice of a family member or friend in a phone call.

27. A core element in this fraud category is romance fraud, whereby offenders construct romantic relationships online with the purpose of deceiving and extorting money from victims. The financial losses to individuals can be significant. It is a problem that impacts on victims in many different regions in the world, and capitalizes on the growth in social networking online and, more specifically, a broader societal trend for finding romantic relationships online. The initial approach to victims is commonly on social media or dating websites and applications by an offender using a false identity along with a corresponding profile narrative. A single offender may switch between identities to target and entice a prospective victim. Once the relationship is established the offender may elicit a financial benefit by initially asking for a small sum of money before asking for larger amounts from the victim, often relaying a crisis scenario that serves to apply pressure and urgency to the victim (e.g. a health emergency or urgent travel requirement). If sexual images were exchanged, money may also be extorted from the victim.

28. A more recent iteration of this method has seen romance fraud converge with cryptocurrency investment fraud. Romance baiting or so-called “pig butchering” fraud – a term whose use is not recommended, out of respect for victims of such crimes – involve an offender fostering a personal relationship with an online victim. Instead of fabricating a crisis scenario, they exploit the intimate relationship and trust to lure them into a fraudulent investment scheme. For offenders, this can incorporate additional stages of planning and preparation, including the development of a fraudulent website or application that can be accessed by the victim, and even the provision of “customer service” for investors.[17] The integration of cryptocurrency investments into the deception has a number of consequences: it widens the prospective pool to include victims from younger age groups; introduces victims to an unfamiliar, volatile and high-risk market, meaning they may be less likely to recognize they are victims; and introduces further difficulties for criminal investigators to trace the funds back to offenders.

[17] Cassandra Cross, “Romance baiting, cryptorom and ‘pig butchering’: an evolutionary step in romance fraud”, *Current Issues in Criminal Justice* (2023); and Fangzhou Wang and Xiaoli Zhou, “Persuasive schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan (杀猪盘) in China”, *Victims and Offenders*, vol. 18, No. 5 (2023).

29. Much of the research into romance fraud has been focused on the victims and their experiences, not the offenders who are less visible. They are considered to be commonly transnational crimes perpetrated by organized criminal groups, with some concentration within certain regions. In the context of "pig butchering" fraud, some organized criminal groups have adopted more elaborate business-like structures in which there is a clear division of labour (e.g. victim contact, information technology and money-laundering) and the recruitment of a workforce of people in need of money and at risk of exploitation, including trafficking in persons.[18]

30. Irrespective of the victims' characteristics, the impact of a relationship and trust fraud can be considerable. While victims experience financial losses, they also suffer from broken trust and the loss of a significant personal relationship. In addition, they experience significant psychological and emotional harm. Some may even refuse to accept that they are or have been a victim of fraud.

E. Fraud involving the impersonation of officials

31. Fraud involving the impersonation of officials, or impersonation fraud, involves the manipulation of communications so that they appear to be from a public or other official, such as the police, a tax authority, a bank or a government department. These frauds employ a range of pretexts and scenarios including the impersonation of a tax authority or other government department claiming an unpaid debt; a bank official claiming money in a bank account is under threat from criminals; or police claiming they have detected a criminal offence by the victim.

32. A key distinguishing feature of impersonation fraud is the use of persuasion techniques that appeal less to the wants and needs of victims (such as in consumer frauds), and instead evoke fear, dread, anxiety and worry. Inducing a heightened emotional state serves to impede decision-making and renders victims more susceptible to manipulation. These messages threaten a negative outcome, including some form of legal response, should the victim not send payment or transfer funds.

33. These frauds commonly involve mass communication such as spam email; communications using social media; text messages; or automated phone calls, or so-called "robodialling", in which phone calls are automated using a recorded message. These technologies facilitate near-simultaneous contact with thousands of victims at a time, giving them immense reach.

F. Identity fraud

34. Identity fraud[19] involves the use of stolen or fake identity information to gain direct access to goods, services or monies from victims, such as the use of stolen information to make purchases or access financial accounts. Identity fraud can be perpetrated without any direct communication or action taken from the individual whose identity is being abused, because the target is often the provider of the goods, services or money. In this way the harm is spread across the different actors who are victimized, including the victim whose identity is abused, the financial service provider or other company from whom the monies are exfiltrated, and in some cases, the provider of the goods or services purchased using the stolen funds.

35. There are different forms of identity information that can be acquired, and each can be exploited in different ways. These include personal information, which comprise individuals' digital identities across different online environments, such as name or date of birth; financial account data, such as credit card numbers; online account information, including usernames and passwords; and biometric data, such as a digital fingerprint stolen from an electronic device.

[18] UNODC, "Casinos, cyber fraud, and trafficking in persons".

[19] See also UNODC *Handbook on Identity-related Crime* (Vienna, 2011).

36. Offenders can access this information by means of system intrusion; social engineering schemes such as phishing or smishing campaigns; or accessing online criminal markets that sell the data. The data can be used to purchase goods and services, submit applications for loans and other finance or access and transfer money from victims' accounts. Additional information on the means includes the following:

(a) System intrusion: some fraudsters are active in the acquisition of personal information by means of illicit hacking techniques, deployment of malware or phishing;

(b) Online criminal markets: there is a vibrant underground economy involved in the buying and selling of identity information, which can be exploited by identity fraudsters. The opportunity to acquire information in this way removes some of the technical barriers for fraudsters who may otherwise not have these capabilities to steal personal information;

(c) Social engineering: this is often achieved by an advertisement or other unsolicited communication sent by email or other online communication, text message or unsolicited phone call, whereby victims are tricked into providing personal information. The degree of sophistication is variable, but more complex methods, such as spoofing legitimate websites can lead to a more significant compromise in providing offenders with direct access to online accounts.

37. There are a range of techniques that are employed by offenders to perpetrate identity fraud. Some of the key methods include account takeover, card-not-present and application fraud, which are defined as follows:

(a) Account takeover: in these frauds, offenders obtain legitimate credentials to access user accounts. These can include bank accounts, but also other types of financial accounts (e.g. virtual currency providers), retail sites or any providers of goods and services. The account can be leveraged for a number of purposes, including directly transferring funds to accounts controlled by the offenders or fraudulently purchasing goods or services using the account. In some instances, acquiring information to access a victim's account marks the first in a sequence of steps required to access the monies, goods or services through subsequent system intrusions. This may involve overcoming security measures such as two-factor authentication. Consequently, offenders resort to additional techniques such as SIM swapping and alternative payment methods;

(b) Card-not-present: unauthorized purchases made remotely from a vendor, either online or over the phone. The acquisition of a victims' financial credentials is sufficient to deceive both the financial service provider and commercial vendor, without the need for a direct interaction with the victim or access to the physical payment card. There are a number of key steps that are typically required by identity fraudsters to exploit a victims' financial credentials:

(i) Acquiring knowledge, resources and financial credentials from online criminal markets;

(ii) Disguising orders to avoid triggering fraud detection algorithms on a commercial site;

(iii) Receiving the orders at an address that cannot be traced to the offenders;

(iv) Reselling the items as an individual seller or selling them in bulk by impersonating a legitimate merchant in mainstream online marketplaces;

(c) Application fraud: these frauds exploit the widespread availability of personal information and use it to apply for credit in the victim's name. This is commonly done with the aim of obtaining a loan from a financial service provider. The offenders are required to access a composite of personal information (e.g. name, address or date of birth) to be able to credibly impersonate the individual. One emerging pattern is the use of technology to create synthetic identities by combining real and fabricated identifiers. Once established these identities can be cultivated over

time to become more creditworthy before eventually submitting applications for high-value financial products.

38. Importantly, the perpetration of identity fraud is not contingent on the involvement of organized crime and organized criminal groups. However, the capacity to perpetrate identity fraud on a large scale and achieve high profits is greatly augmented by the skills and resources available to organized crime. This threat is rendered particularly acute by the proliferation of available online targets within growing digital economies. The manipulation and abuse of identity can serve a variety of functions in the commission of organized crime, including efforts to trace the criminal activity back to the perpetrators.[20]

G. Fraud against businesses or organizations

39. Fraud against businesses or organizations typically involves the abuse of internal systems or a commercial relationship to defraud the victim. These frauds can be perpetrated by someone either internal or external to the organization. Some are perpetrated by otherwise legitimate enterprises and actors or using legitimate products, rather than being schemes that are designed from the outset to perpetrate a fraud, sometimes in response to internal pressures or dubious work practices or culture.

40. Some examples of fraud against businesses or organizations include:

(a) Business email compromise fraud is a cyber-enabled fraud that is perpetrated in high volumes. Businesses and organizations of all sizes and from a range of sectors fall victim to this type of fraud, commonly committee by external criminals. The offenders infiltrate systems and use social engineering techniques to persuade personnel to make unauthorized transfers of funds to accounts in the control of the offenders. The losses to victims can be very high. A first step is to infiltrate the communication systems of an organization to help persuade the recipients that they are legitimate. Key methods include hacking the email accounts of staff members; sending phishing emails to elicit the account details of staff members; or exploiting communication providers to impersonate domain names that are familiar to the target organization.[21] There are various narratives that are adopted by offenders, which include exploiting an existing relationship between two companies by issuing a fake invoice; sending an email purporting to be from a senior staff member that presents an urgent request for funds; or impersonating a lawyer requesting a wire transfer to address a sensitive matter.[22] Communication can occur over a period of time and the offenders may invest time to understand the organization and its systems and victimize them on multiple occasions;

(b) Financial statement frauds include a multitude of methods in which otherwise legitimate professionals in a financial market mislead and distort the perceptions of others such as investors, regulators and other market actors about the financial health and future prospects of a company or fund. Similar types of accounting fraud may also cover up the misappropriation, misapplication or embezzlement of funds. These frauds can be perpetrated in response to pressures to meet performance expectations. Examples include corporate executives, rogue financial traders or hedge fund managers reporting on financial performance. In some

[20] Simon Baechler, “Document fraud: will your identity be secure in the twenty-first century?”, *European Journal on Criminal Policy and Research*, vol. 26, No. 3 (June 2020).

[21] Norah Saud Al-Musib and others, “Business email compromise (BEC) attacks”, *Materials Today: Proceedings*, (vol. 81, Part 2 (2023)); and Geoffrey Simpson, Tyler Moore and Richard Clayton, “Ten years of attacks on companies using visual impersonation of domain names”, research paper presented at the Symposium on Electronic Crime Research (eCrime), hosted by the Anti-Phishing Working Group and held in Boston, United States of America, from 16 to 19 November 2020.

[22] Alessandro E. Agazzi, “Business Email Compromise (BEC) and cyberpsychology”. Available at https://arxiv.org/; and Al-Musib and others, “Business email compromise (BEC) attacks”.

cases the impact of these frauds is felt outside of the business, including external businesses, sectors or even the wider economy;[23]

(c) Long or short firm frauds can be perpetrated by existing trading companies or companies that may have been procured or set up for a fraudulent purpose. The companies establish a credit history, trust or credibility, which is used to deceive a buyer, seller or creditor into supplying goods or finance. The firms do this knowing either that they cannot pay or have no intention of making payment.

III. Topics for consideration

41. The Working Group may wish to focus its deliberations on the following topics:

(a) The nature of organized fraud in various jurisdictions;

(b) The use of the Organized Crime Convention to prevent and combat organized fraud, as well as the criminalization of fraud as serious crime, as defined in article 2 of the Convention;

(c) Opportunities for effective international cooperation, including with the private sector;

(d) Information-sharing on the prevention of organized fraud, the protection of fraud victims and witnesses, as well as whistle-blowers, and the pursuit of organized criminal groups involved in organized fraud, as well as the promotion of partnerships with those aims;

(e) Identification of relevant technical assistance needs relating to the implementation of the Organized Crime Convention to prevent and combat organized fraud.

IV. Follow-up and possible recommendations

42. The Working Group may wish to make the following recommendations:

(a) Encourage States parties that have not yet done so to consider criminalizing fraud as serious crime, as defined in article 2, paragraph (b), of the Organized Crime Convention, in order to ensure that, where the offence is transnational in nature and involves an organized criminal group, effective international cooperation can be afforded under the Convention;

(b) Urge States parties to use the tools offered by the Organized Crime Convention to develop or amend national legislation, as necessary and appropriate, to prevent and combat fraud, including fraud committed by organized criminal groups;

(c) Encourage States parties to analyse, in consultation with other relevant stakeholders, where appropriate, trends in activities of organized criminal groups with respect to organized fraud and to share that information and data with the United Nations Office on Drugs and Crime;

(d) Request the United Nations Office on Drugs and Crime, subject to the availability of extrabudgetary resources, to collect, analyse and disseminate information regarding organized fraud;

(e) Urge States parties to provide one another with the widest measure of international cooperation, including mutual legal assistance, in investigations, prosecutions and judicial proceedings in relation to organized fraud and related offences covered by the Organized Crime Convention and the Protocols thereto;

[23] United Kingdom of Great Britain and Northern Ireland, Serios Fraud Office, “Senior bankers sentenced to 9 years for rigging EURIBOR rate”, 1 April 2019.

(f) Encourage States parties to strengthen their cooperation with relevant stakeholders, including the private sector, civil society organizations, the media, academia and the scientific community, in preventing and combating organized fraud, including through education and awareness-raising campaigns;

(g) Request the United Nations Office on Drugs and Crime, subject to the availability of extrabudgetary resources, to continue to develop technical assistance tools, and to provide technical assistance, including capacity-building, upon request, for purposes of supporting States parties in efforts to effectively implement the Organized Crime Convention in preventing and combating organized fraud;

(h) Request States parties that have not yet done so to update their legislative records on the criminalization of organized fraud in the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.