

# ORGANIZED FRAUD

ISSUE PAPER



## **ISSUE PAPER**

## ORGANIZED FRAUD



#### Acknowledgements

The present issue paper was prepared by the Conference Support Section, Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs of the United Nations Office on Drugs and Crime (UNODC).

#### Research and drafting

The present issue paper was drafted by Michael Skidmore, consultant. UNODC wishes to acknowledge the contributions of Ramy Abdelhady, Victoria Luján Ecarri, Roxana-Andreea Mastor and Riikka Puttonen, of the Conference Support Section, who contributed to the development of the issue paper. The issue paper benefited from the valuable contributions of many UNODC staff members who reviewed and provided input for various sections, including Loide Aryee, Renata Delgado-Schenk, Giovanni Gallo, Magdalena Howland, Theodore Leggett, Glen Prichard, Jason Reichelt, Tim Steele and Woody Tan.

#### Contributions

Other individuals and organizations contributed to the preparation of the present issue paper. UNODC acknowledges with profound gratitude those who shared their expertise and experience during the international meeting of experts held in person in Vienna and online from 4 to 6 March 2024: Jorij Abraham (Global Anti-Scam Alliance), Bina Bhardwa (Institute for Crime and Justice Policy Research), Muhammad Bin Mohamed Farid (Singapore), Sebastian Bley (European Union Agency for Law Enforcement Cooperation), Mark Button (University of Portsmouth, United Kingdom of Great Britain and Northern Ireland), Mina Chiang (Humanity Research Consultancy), Nicholas Court (International Criminal Police Organization (INTERPOL)), Ian Dyson (United Kingdom), Richard Goldberg (United States of America), Cosmin-Adrian Iordache (European Public Prosecutor's Office), Eric Kasper (Humanity Research Consultancy), Jeanette Kroes (INTERPOL), Dexter Laggui (Philippines), Michael Levi (Cardiff University, United Kingdom), Nicholas Lord (University of Manchester, United Kingdom), Mary Rose Magsaysay (Philippines), Rafael Henrique Martins Fernandes (Brazil), Jennifer Mendez (American Society of International Law), Daniel Mostardeiro Cola (Brazil), Olegs Olins (Latvia), Christopher Omahi Ogbaji (Nigeria), Sophia Rowe (Jamaica), Kien Soloman (United Kingdom), Victoria Ugo-Ali (Nigeria), Dan Joshua Valenton (Philippines), Thomas Von der Gathen (Payment Services Austria), Xiumei Wang (Beijing Normal University), Kathy Waters (Advocating Against Romance Scammers) and Robin Tim Weis (Zero Project).

The publication of the present issue paper was supported through a financial contribution from the Government of the United Kingdom. The content of the issue paper is the sole responsibility of UNODC and does not necessarily reflect the views of the Government of the United Kingdom.

© United Nations, 2024. All rights reserved.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Information on uniform resource locators and links to Internet sites contained in the present publication are provided for the convenience of the reader and are correct at the time of issue. The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

Publishing production: Publishing Section, United Nations Office at Vienna.

## CONTENTS

	Page
Acknowledgements	ii
Introduction	1
Scope of the issue paper	2
Methodology	
Structure of the issue paper	
Chapter I. Principles for understanding organized fraud	7
Defining fraud	7
Organized criminal groups in the context of fraud	
Serious crime in the context of fraud	
Intersectionality	18
Chapter II. Categories of organized fraud	21
Consumer products and services fraud	22
Employment fraud	25
Consumer investment fraud	26
Fraud by impersonation of a trusted individual or organization	28
Identity fraud	30
Relationship and trust fraud	34
Fraud against businesses or organizations	36
Chapter III. Organized fraud offenders	41
Role and significance of co-offending	41
Characteristics of organized fraud offenders	43
Motivations of fraudsters	45
Chapter IV. Cross-cutting facilitators of organized fraud	49
Mass-marketing	49
Identity theft	50
Money-laundering	52
Enabling technology	55
Chapter V. Tackling organized fraud	59
Prevention of organized fraud	61
Pursuit of organized criminal groups	62
Protection of persons affected by organized crime	67
Promotion of partnerships and cooperation	68
Conclusion	73



## Introduction

Fraud has evolved significantly over the years, adapting to technological advancements and changes in society. It has become increasingly sophisticated, often using psychological manipulation, enabled by information and communications technologies (ICTs). The high volume and severity of fraud pose a significant risk to people, economies and prosperity worldwide, and have a negative impact on 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, selfblame 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.<sup>2</sup> The anonymity and remoteness often associated with fraud perpetration conceal the identities of offenders from both victims and authorities, hindering efforts to assess underlying patterns, factors of vulnerability and associated risks. Furthermore, the dynamic nature of fraud — which is constantly being adapted to changes in legal, social, commercial and technological systems — means that new and innovative methods of the offence may go unnoticed within static official data. In many cases, domestic law enforcement entities do not have the capacity to investigate and uncover the offenders and the organized criminal groups behind the crime:<sup>3</sup> international cooperation is required, suggesting the need to give greater prominence to fraud in the policy framework and legislation against organized crime.4

The international community has recognized the worrying scale of fraud and the need for joint efforts in preventing and combating it.<sup>5</sup> The General Assembly, in its resolution <u>78/229</u>, reaffirmed the importance of the work of the United Nations Office on Drugs and Crime (UNODC) in the fulfilment of its mandate in crime prevention and criminal justice, including providing to Member States, upon request and as a matter of high priority, technical cooperation, advisory services and other forms of assistance, and coordinating with and complementing the work of all relevant and competent United Nations bodies and offices in respect to all forms of organized crime, including

<sup>&</sup>lt;sup>1</sup> Mark Button, Christopher Lewis and Jacki Tapley, "Not a victimless crime: the impact of fraud on individual victims and their families", Security Journal, vol. 27, No. 1 (February 2014).

<sup>&</sup>lt;sup>2</sup> Cynthia Courtois and Yves Gendron, "Research: why corporate fraud reports are down", *Harvard Business Review*, 1 July 2020.

<sup>&</sup>lt;sup>3</sup> Analysis of crime data in the United Kingdom of Great Britain and Northern Ireland explored the links between fraud offences reported by the public and organized crime and estimated that at least 31 per cent could be attributed to organized crime. This was based on several characteristics, including the involvement of co-offenders, repeat offending, the theft of large amounts of money and the level of sophistication (e.g. planning or technical skill). However, interpretation is challenged by the limited contextual information on the offenders and underlying criminal processes and a lack of conceptual clarity for drawing firm lines around fraud that can be attributed to organized crime (see Ruth Crocker and others, *The Impact of Organized Crime in Local Communities* (London, The Police Foundation, 2017)).

<sup>&</sup>lt;sup>4</sup> Hans-Jörg Albrecht, "Police, policing and organized crime: lessons from organized crime research", in *European Law Enforcement Research Bulletin*, Special Conference Edition No. 2, Detlef Nogala and others, eds. (Luxembourg, Publications Office of the European Union, 2017); and Michael Levi, Ognian Shentov and Boyko Todorov, eds., *Financing of Organised Crime* (Sofia, Center for the Study of Democracy, 2015).

<sup>&</sup>lt;sup>5</sup>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.

fraud. Nevertheless, the intersection between fraud and organized crime is not well understood and is further complicated by overlaps with other key areas, including cybercrime, white-collar crime, money-laundering and corruption. An understanding of organized fraud is necessary to inform the decisions of policymakers and other stakeholders and drive effective responses. The United Nations Convention against Transnational Organized Crime, the main global legally binding instrument to prevent and fight all forms and manifestations of transnational organized crime and protect the victims thereof, provides a framework to understand the nature of organized fraud and how the response to it can be integrated into the response to the different threats presented by transnational organized crime.

#### Scope of the issue paper

Fraud is an expansive category of crime. One of the greatest challenges to understanding it is its scope. It encompasses a range of criminal behaviours that are bound together by the common principle of dishonesty. The opportunities to employ dishonesty for the purposes of fraud span the full range of social, commercial, financial and technological settings, which can vary in different regions of the world. These opportunities are exploited by criminals from highly diverse backgrounds, ranging from professionals exploiting a legitimate corporate position to cybercriminals from within deprived communities. In this way, fraud is distinct from many other criminal categories that cover more discrete criminal behaviours occurring in specific settings (e.g. burglary). This diversity creates challenges in terms of developing a single, cohesive and comprehensive picture of fraud.

The present issue paper covers fraud perpetrated by organized criminal groups (i.e. organized fraud). The role of organized crime can vary depending on the type of fraud, although, to a greater or lesser extent, it has a footprint in nearly all types of fraud. For the purposes of containing the scope of the issue paper, the following elements are not included:

- Other crimes in which fraud plays an enabling role, including the fraudulent use of identity
  to prevent a perpetrator from being traced, such as opening financial accounts to launder
  the proceeds of crime;<sup>9</sup> fraudulent communications to enter into a relationship with a
  victim for the purpose of blackmailing or extorting money from them;<sup>10</sup> and fraudulent job
  advertisements for recruiting and trafficking victims into forced labour and servitude.<sup>11</sup>
- Fraud targeting the financial interests of the State (e.g. tax regimes), such as missing trader intra-community fraud (otherwise known as MTIC or VAT fraud); excise fraud, in which duties on imported products are not paid (e.g. fuel); public procurement fraud; and fraudulent

<sup>&</sup>lt;sup>6</sup> Jay S. Albanese, "Organized crime as financial crime: the nature of organized crime as reflected in prosecutions and research", *Victims and Offenders*, vol. 16, No. 3 (2021); and Andrea Di Nicola, "Towards digital organized crime and digital sociology of organized crime", *Trends in Organized Crime* (2022).

<sup>&</sup>lt;sup>7</sup> Michael Levi, "Organized fraud and organizing frauds: unpacking research on networks and organization", *Criminology and Criminal Justice*, vol. 8, No. 4 (November 2008). See also International Criminal Police Organization (INTERPOL), "INTERPOL global financial fraud assessment" (Lyon, France, 2024).

<sup>&</sup>lt;sup>e</sup> See, for example, Arjan Reurink, Financial Fraud: A Literature Review, MPIfG Discussion Paper, No. 16/5 (Cologne, Germany, Max Planck Institute for the Study of Societies, 2016); and Mikol A. Mortley, "A crime of opportunity: an analysis of the Jamaican lottery scam" [Kingston, 2017].

<sup>&</sup>lt;sup>9</sup> 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 (September 2020).

<sup>&</sup>lt;sup>10</sup>Anna Coluccia and others, "Online romance scams: relational dynamics and psychological characteristics of the victims and scammers – a scoping review", *Clinical Practice and Epidemiology in Mental Health*, vol. 16 (2020).

<sup>&</sup>lt;sup>11</sup> Global Report on Trafficking in Persons 2022 (United Nations publication, 2022), p. 102. For further information, see the section on employment fraud in chapter II of the present issue paper; and INTERPOL, "INTERPOL global financial fraud assessment", p. 20.

applications for government grants and subsidies.<sup>12</sup> The policy and response landscape for addressing these types of fraud can be distinct, being made up of various agencies and regulatory powers beyond law enforcement (e.g. the tax authority).<sup>13</sup> The links between these types of fraud and organized crime are more well established in the literature.<sup>14</sup>

The focus of the issue paper is organized fraud that targets individual members of the public or private institutions for the purposes of obtaining a financial or other material benefit.

#### Methodology

#### Developing a typology

There are a multitude of principles that can be adopted to represent the different dimensions of fraud. They might include the key underlying technical or criminal enablers that provide the tools to perpetrate fraud, for example, the key methods for exploiting communications channels such as telecommunications or online advertising, 15 and processes of hacking, identity theft or social engineering. 16 Arranging knowledge of fraud according to these principles may provide insights into the underlying processes that drive fraud offending behaviour; however, the visibility of these different elements can be limited. This is because victims who report the crimes often do not know how the fraud was perpetrated. 17 Furthermore, some underlying enablers drive multiple forms of crime; for example, hacking and system intrusion can be a precursor to fraud, but also other categories of crimes (e.g. blackmail in ransomware attacks).

The fraud categories developed for the present issue paper take a victim-centred perspective, and therefore have a primary focus on the narrative or ruse that is presented to the victims (e.g. the investment or romance). In this context, the issue paper builds on previous work that adopts similar principles for developing a fraud typology based on victims and their experiences, such as a typology to reflect the victim's expected or promised reward, benefit or outcome from the fraudulent communication. There are convergences in the methods underlying victim-based categories, with commonalities in the technologies and deception techniques used by the offenders engaged in the different types of fraud. Some criminals may engage in multiple types of fraud as part of a single fraudulent scheme or employ similar techniques to engage in different types of fraudulent scheme.

<sup>&</sup>lt;sup>12</sup>Shann Hulme, Emma Disley and Emma Louise Blondes, eds., *Mapping the Risk of Serious and Organised Crime Infiltrating Legitimate Businesses: Final Report* (Brussels, Publications Office, 2021); European Union Agency for Law Enforcement Cooperation (Europol), *Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (The Hague, 2017); and Europol, *Online Fraud Schemes: A Web of Deceit*, Europol Spotlight Report Series (Luxembourg, Publications Office of the European Union, 2023).

<sup>&</sup>lt;sup>13</sup> Mark Button, David Shepherd and Dean Blackbourn, *The Fraud "Justice Systems": A Scoping Study on the Civil, Regulatory and Private Paths to "Justice" for Fraudsters – Main Report* (Portsmouth, United Kingdom, University of Portsmouth, 2016).

<sup>&</sup>lt;sup>14</sup>Hulme, Disley and Blondes, eds., *Mapping the Risk of Serious and Organised Crime*.

<sup>&</sup>lt;sup>15</sup>For example, David Ng'ang'a Njuguna, John Kamau and Dennis Kaburu, "A review of smishing attacks mitigation strategies", *International Journal of Computer and Information Technology*, vol. 11, No. 1 (February 2022); Jean-Loup Richet, "How cybercriminal communities grow and change: an investigation of ad-fraud communities", *Technological Forecasting and Social Change*, vol. 174, art. No. 121282 (January 2022); and Shadi Sadeghpour and Natalija Vlajic, "Ads and fraud: a comprehensive survey of fraud in online advertising", *Journal of Cybersecurity and Privacy*, vol. 1, No. 4 (December 2021).

<sup>&</sup>lt;sup>16</sup> Jason R.C. Nurse, "Cybercrime and you: how criminals attack and the human factors that they seek to exploit", in *The Oxford Handbook of Cyberpsychology*, Alison Attrill-Smith and others, eds. (Oxford, Oxford University Press, 2019).

<sup>&</sup>lt;sup>17</sup> Mark Button and others, "Online frauds: learning from victims why they fall for these scams", *The Australian and New Zealand Journal of Criminology*, vol. 47, No. 3 (December 2014).

<sup>&</sup>lt;sup>18</sup>The issue paper draws on previous research that has sought to delineate the different categories of fraud targeted at individuals and/ or businesses, such as Michaela Beals, Marguerite DeLiema and Martha Deevy, "Framework for a taxonomy of fraud" (Stanford, California, Stanford Center on Longevity, 2015); and Michael Levi and John Burrows, "Measuring the impact of fraud in the UK: a conceptual and empirical journey", *The British Journal of Criminology*, vol. 48, No. 3 (May 2008).

One category included in the typology is fraud that targets businesses and organizations. This reflects a category of victim rather than a specific narrative or ruse, and thereby incorporates diverse fraudulent schemes and methods. These types of fraud were consolidated to ensure that businesses and organizations are recognized as a key victim group.

These categories are presented as an initial step to developing a common language and understanding of the different categories of organized fraud. The categories are not necessarily the preserve of organized criminal groups, but each category will be discussed in the context of organized fraud. Some categories are more expansive than others, with a multitude of subcategories, some of which are discussed in a non-exhaustive way in the issue paper.

#### Literature review

The present issue paper presents exploratory research to examine the nature of organized fraud as experienced across different regions of the world. It contains a compilation and review of information from academic journal articles, policy papers and publications.

A search of online sources was completed to identify publications covering organized fraud offending or offenders. The subject of organized fraud, or organized crime in the context of fraud, has received limited coverage in the existing literature. The issue paper contains a synthesis of evidence collected in multiple related criminological fields, including fraud, organized crime and cybercrime. The paper does not contain a systematic review of the literature but is rather a targeted analysis of key literature aimed at representing and illustrating some of the primary themes.

#### Case studies

Case studies were collected to provide illustrative examples of organized fraud from the different regions of the world and to capture new and emerging methods and technologies. The case studies were taken from a range of sources, including the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal, academic papers, policy reports and legal research.

Preliminary research on fraud legislation in 37 countries across all regions of the world was undertaken, with a particular focus on legal definitions and frameworks guiding the decisions on sentencing for convicted offenders. There may be elements of fraud in the legislation of other countries that are not considered here.

#### Limitations of the review

In many official sources and research papers, fraud is examined through the lens of law enforcement and official data. Fraud is widely underreported and, therefore, some caution is needed in interpreting the problem and developing solutions on the basis of incomplete data. The present issue paper contains a compilation of research from a range of regions, but availability was varied, and in some regions the research was more limited or nascent. Consequently, the extent to which the evidence included in the issue paper represents the patterns in organized fraud across all regions is not known. There is also currently a gap in data on organized fraud disaggregated by factors such as disability, age, gender and economic status, which limits the analysis and understanding of the enablers of targeting victims and perpetrating organized fraud.

#### Structure of the issue paper

The issue paper is structured as follows:

- Chapter I sets out the principles for understanding organized fraud, examining the definition of fraud, and key aspects of the Organized Crime Convention.
- Chapter II provides a typology of organized fraud, with an in-depth description of each category.
- Chapter III contains a discussion of organized fraud offenders, examining their profiles and the pathways that they take into organized fraud offending.
- Chapter IV contains a description of the cross-cutting facilitators of fraud, including some of the key technologies and behaviours that enable organized fraud.
- Chapter V discusses national and international responses, key considerations, gaps and areas for improving prevention and law enforcement.



## CHAPTER I

# Principles for understanding organized fraud

Before focusing on the typology of organized fraud, the present chapter addresses some general considerations around the definition of fraud, the Organized Crime Convention, and fraud in the context of organized crime.

## Defining fraud

There is no single definitive understanding of the behaviours that make up fraud. Some have defined fraud in very broad terms, for example, "obtaining something of value or avoiding an obligation by means of deception". <sup>19</sup> Others have provided more elaborate definitions to describe in more specific terms the composite behaviours that are represented by fraud, including highlighting the purposeful intent and violation of trust. <sup>20</sup> INTERPOL has emphasized the deliberate element implied in the term "deception", reinforcing the significance of intent in defining fraud, and defines fraud as the "aim at the procurement of a financial gain through deliberate, deceitful actions against individuals and to their detriment". <sup>21</sup>

Similarly, there is no single legal definition of fraud, and the variable definitions across legal jurisdictions, or in different statutes, evoke only a broad concept of fraud.<sup>22</sup> Under countries' criminal laws, fraud is described in different ways and to varying degrees of specificity.<sup>23</sup> Some laws provide a generalized description of the behaviours that constitute fraud,<sup>24</sup> whereas others make reference to certain activities, products or services that are prominent in fraudulent schemes, such as the impersonation of a trusted entity or the manipulation or unauthorized use of data.<sup>25</sup> Some States have introduced separate

<sup>&</sup>lt;sup>19</sup> Grace 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), p. 1. See also Michael Levi, "Financial crimes", in *Oxford Handbook of Crime and Public Policy*, Michael Tonry, ed. (New York, Oxford University Press, 2009), pp. 223–246.

<sup>&</sup>lt;sup>20</sup> Reurink, Financial Fraud.

<sup>&</sup>lt;sup>21</sup> INTERPOL, "INTERPOL global financial fraud assessment", p. 5.

<sup>&</sup>lt;sup>22</sup> Alan Doig, Fraud (Cullompton, United Kingdom, Willan, 2006); and Reurink, Financial Fraud.

<sup>&</sup>lt;sup>23</sup> For the purposes of the present paper, the legal definitions in 37 countries in all regions of the world were examined.

<sup>&</sup>lt;sup>24</sup> See, for example, the legislative examples for Spain and Uruguay included in the present section.

 $<sup>^{25}</sup>$  For example, in Algeria, fraud is defined as the receipt of money by means of using a false identity or the names of others, such as the authorities, or by persuading an individual of something that is untrue, such as a lottery win or the occurrence of an accident.

legislation to address different facets of fraud offending, for example, computer fraud or fraud against credit, businesses and auctions.<sup>26</sup>

There are some core elements of fraud that feature in most legal definitions: using deception to gain an unjust advantage or benefit and causing a detriment to another person or organization. Deception is variously described as dishonesty, false (or mis-) representation, 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.

The definitions below are taken from Spain and Uruguay and provide examples of two broad definitions of fraud that have been adopted in law.

#### LEGISLATIVE EXAMPLE: SPAIN



#### ORGANIC ACT NO. 10/1995 - CRIMINAL CODE

Article 248.1. Any person who, for gain, uses deception that is sufficient to lead another person to carry out, in error, an act of disposition that is detrimental to him- or herself or to another, shall be guilty of fraud.

#### LEGISLATIVE EXAMPLE: URUGUAY



#### **CRIMINAL CODE NO. 9155**

Article 347. Any person who, by means of artifice or deception, tricks another person in order to obtain for him- or herself or for a third person an undue advantage, to the detriment of another, shall be punishable by imprisonment for a term of six months to four years.

In the present issue paper, a broad definition of fraud is adopted to encompass the variants described in the laws of different countries. It includes fraud that deliberately uses deception, <sup>27</sup> by any method<sup>28</sup> or medium, <sup>29</sup> with the intent to make a wrongful financial or other material gain, <sup>30</sup> and which causes a detriment to another. <sup>31</sup>

One final point to acknowledge in defining fraud is the fine line that can separate a criminal and civil matter – particularly in cases where intent is difficult to discern – and there can be challenges for law enforcement entities in determining that a crime has occurred.<sup>32</sup> Furthermore, a perpetrator may be sanctioned using a range of criminal, civil or administrative penalties depending on the nature of the

<sup>&</sup>lt;sup>26</sup> For example, in the Republic of Korea, there is separate legislation for fraud that is detrimental to the credit of another and for fraud by use of a computer (e.g. the false inputting of data in identity fraud).

<sup>&</sup>lt;sup>27</sup> This includes the use of false names, qualities or enterprises or the making of false statements that abuse trust and instil confidence, a false hope or fear of an event that is not real to induce another person to part with his or her own or another's money or to surrender a legal or property right or any material benefit. This also includes the deliberate concealment of material facts.

<sup>&</sup>lt;sup>28</sup> For example, through the use of false documents or by inputting false data or giving unauthorized commands to a computer.

<sup>&</sup>lt;sup>29</sup> This includes fraud perpetrated online, by telephone, by mail or in person, or a combination of these.

<sup>&</sup>lt;sup>30</sup>This includes the obtainment, or attempt to obtain, funds, access to services, fixed or movable property, bonds, bills, promises, receipts or discharges or a release from obligations.

<sup>&</sup>lt;sup>31</sup> This detriment can be to an individual, a business or an organization and includes losses of any value or significance to the victim.

<sup>&</sup>lt;sup>32</sup>To illustrate, in the context of investment fraud, malpractice can range from outright deception to neglectful practices and the provision of poor information to clients. Furthermore, the anticipated benefit could be many years into the future and therefore it can be difficult to substantiate that it will not deliver what was promised, and thereby establish criminal intent (Michael Skidmore, *Protecting People's Pensions: Understanding and Preventing Scams* (London, The Police Foundation, 2020)).

fraud and the surrounding regulatory provisions available in the public or private sector.<sup>33</sup> Given its focus on organized crime, fraud for which there is criminal liability is covered in the present issue paper, but it is noted there will be variability in the different national jurisdictions.<sup>34</sup>

The wider theme of cybercrime features prominently in fraud, although there is no single approach for defining fraud in the context of cybercrime.<sup>35</sup> One way to understand cybercrime is to examine how and to what extent a crime has been transformed by ICT.<sup>36</sup> ICT-related fraud is commonly described as a cyber-enabled crime,<sup>37</sup> in that it is traditional crime that uses ICT systems to increase its scale and reach. It is thus different from cyber-dependent crimes, which can be committed only through the use of ICT systems and which target the integrity, availability and confidentiality of electronic data and ICT systems.<sup>38</sup> However, this dichotomy ignores the various ways in which cyber-dependent crime intersects with fraud, particularly when viewed from the perspective of offenders and the sequence of underlying offences in the commission of fraud, for example, gaining illegal access to an ICT system for perpetrating business email compromise fraud. There are frameworks that conceptualize cybercrime as a continuum, ranging from crimes that are wholly technology-based to crimes in which the use of ICT systems is incidental.<sup>39</sup> The use of ICT systems for perpetrating fraud is highly variable and spans much of this continuum. The present issue paper contains the term "cyberfraud", which represents all types of fraud on this continuum.

## Organized criminal groups in the context of fraud

Fraud encompasses offending that is wide-ranging in method, sophistication and impact. It encompasses offenders ranging from opportunistic individuals who make moderate financial gains to highly motivated and organized criminals who go to great lengths to orchestrate fraud to make staggering levels of criminal profit. <sup>40</sup> Thus, the line separating fraud that is organized and that which is not can be difficult to draw. Therefore, clearer distinctions would help in developing policies and responses that are more firmly aligned with the designated problem.

An "organized criminal group" is defined in article 2 (a) of the Organized Crime Convention as a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with the Convention, in order to obtain, directly or indirectly, a financial or other material benefit. Article 2 (c) of the Convention also provides further clarification as to the meaning of a "structured group". These definitions incorporate flexibility for law enforcement entities to identify and address organized criminal

<sup>&</sup>lt;sup>33</sup> Mark Button and others, Fraud and Punishment: Enhancing Deterrence Through More Effective Sanctions – Main Report (Portsmouth, United Kingdom, University of Portsmouth, 2012).

<sup>34</sup> Reurink, Financial Fraud.

<sup>&</sup>lt;sup>35</sup> Alisdair A. Gillespie and Samantha Magor, "Tackling online fraud", ERA Forum: Journal of the Academy of European Law, vol. 20. No. 3 (2019).

<sup>&</sup>lt;sup>36</sup> David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, United Kingdom; Malden, Massachusetts, United States of America, Polity Press, 2007).

<sup>&</sup>lt;sup>37</sup> The terms "cyber-enabled crimes" and "cyber-dependent crimes" are used for illustrative purposes only. There is no agreement at the international level on their exact content and usage.

<sup>&</sup>lt;sup>38</sup> For examples of cyber-enabled and cyber-dependent crimes, see Mike McGuire and Samantha Dowling, *Cyber Crime: A Review of the Evidence – Summary of Key Findings and Implications*, Home Office Research Report, No. 75 (2013).

<sup>&</sup>lt;sup>39</sup> Sarah Gordon and Richard Ford, "On the definition and classification of cybercrime", *Journal in Computer Virology*, vol. 2, No. 1 (August 2006); and Kirsty Phillips and others, "Conceptualizing cybercrime: definitions, typologies and taxonomies", *Forensic Sciences*, vol. 2, No. 2 (April 2022).

<sup>&</sup>lt;sup>40</sup> See also Jonathan M. Karpoff, "The future of financial fraud", *Journal of Corporate Finance*, vol. 66 (2021); and Levi, "Organized fraud and organizing frauds".

groups. The structure that a group needs to take is not specified in the Convention, nor is the time period over which the group needs to have existed.<sup>41</sup>

Offenders in organized criminal groups are structured in diverse ways. Such groups include those that operate in a more rigid hierarchy, those with horizontal structures that coalesce around a core group of individuals and networks that involve shifting alliances of individual criminals who do not perceive themselves as a group but still fall under the definition.

The conventional stereotypical attributes associated with organized crime are not always essential to the perpetration of organized fraud,<sup>42</sup> and the business models and structures adopted by organized criminal groups must be considered in relation to the environments where criminal opportunities arise, the methods used and the skills needed:

- Fraud is primarily concerned with monetary theft rather than the production or distribution of illegal goods, distinguishing it from other organized criminal activities.
- Many fraudulent activities are carried out remotely, facilitated by technology that enables
  anonymous communication and the transfer of stolen funds across national borders, and
  victims and offenders seldom need to be in the same place at the same time.
- Fraud often relies on victims willingly providing access to their funds, instead of the use of force
  or coercion, with success hinging on deceitful tactics that can blur the line between legitimate
  and illegitimate entities.
- White-collar fraud is perpetrated from within otherwise legitimate organizations and occupations.

There is no typical structure for an organized criminal group involved in fraud and, as with other forms of organized crime, there is regional variation in the methods and structures employed by organized criminal groups. <sup>43</sup> This is in part because there is such a diverse array of opportunities to perpetrate serious fraud that emerge within global and interconnected business, financial and commercial settings. The organization of these crimes and the perpetrators thereof take many different forms when such groups seek to exploit these opportunities. The emergence of organized crime in different regions reflects the contingent relationships between different global settings, the capacity of would-be fraudsters in a population to identify and act on criminal opportunities and the controls put in place by the State or others to prevent these crimes. <sup>44</sup>

Research on the ways in which organized criminal groups take shape in the context of fraud is still developing, but an understanding of their different manifestations is an important step in identifying and prioritizing the most serious fraudsters for law enforcement intervention.<sup>45</sup>

<sup>&</sup>lt;sup>41</sup> A multitude of definitions of organized crime are applied in the research literature, some of which specify activities such as violence, corruption or the infiltration of the legitimate economy as intrinsic to the presence of organized crime. For example, one study highlighted the absence of these activities among cyberfraudsters and thus questioned the role that "organized crime" played in those crimes (Eric Rutger Leukfeldt, Anna Lavorgna and Edward R. Kleemans, "Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime", *European Journal on Criminal Policy and Research*, vol. 23, No. 3 (September 2017)).

<sup>&</sup>lt;sup>42</sup> Kim-Kwang Raymond Choo and Russell G. Smith, "Criminal exploitation of online systems by organised crime groups", *Asian Journal of Criminology*, vol. 3, No. 1 (June 2008); Levi, "Organized fraud and organizing frauds"; and Di Nicola, "Towards digital organized crime".

<sup>&</sup>lt;sup>43</sup> INTERPOL, "INTERPOL global financial fraud assessment".

 $<sup>^{\</sup>rm 44}\,\mathrm{Levi},$  "Organized fraud and organizing frauds".

<sup>&</sup>lt;sup>45</sup> Importantly, the perpetration of serious fraud is not always contingent on having co-offenders. Examples include professionals who abuse a legitimate position or those able to exploit technology to automate offending (Levi, "Organized fraud and organizing frauds"; and Wystke van der Wagen and Wolter Pieters, "From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks", *British Journal of Criminology*, vol. 55, No. 3 (May 2015)).

The perpetration of fraud entails a complex series of events to plan, execute and finalize criminal activity to access funds and avoid detection by the authorities. <sup>46</sup> Fraud can be transnational, occur over an extended period of time, reach a multitude of victims and involve processes of money-laundering and corruption in the public or private sectors. <sup>47</sup> Co-offenders are often necessary to complete the complex series of events. Some are recruited to provide specific capabilities that can augment the capacity and scope to perpetrate fraud, whereas others are required to undertake labour-intensive tasks. Examples include the recruitment of legitimate professional enablers, cybercriminals with access to technical knowledge and resources and telephone operators who undertake telemarketing. <sup>48</sup> Co-offenders in organized criminal groups perform various functions depending on the specific requirements of a fraud scheme, and they can vary in their importance, awareness and involvement. <sup>49</sup>

The nature of the relationships among co-offenders within different organized criminal groups can vary depending on how the relationships are formed and for what purpose. Some organized criminal groups foster durable social bonds between co-offenders, whereas in others, the relationships are formed for the more singular and pragmatic purpose of successfully committing a crime. The ways in which these relationships take shape can affect the structure and stability of the organized criminal group, and this variation is evident in the context of organized fraud.

Organized criminal groups that engage in other forms of serious crime can be attracted to the high profits and relatively low risks involved in the perpetration of fraud.<sup>51</sup> They are often durable groups that can leverage criminal ties and resources to facilitate the commission of large-scale fraud. This can include the capacity to exert influence over others in both legitimate society and the criminal underworld.<sup>52</sup> In some regions, organized criminal groups offer protection and security to insulate local fraud offenders from the threat of local law enforcement entities or other criminals.<sup>53</sup> A key example is the so-called scam compounds operated by poly-criminal groups in South-East Asia, which have industrialized processes for perpetrating certain types of fraud (e.g. romance fraud), in part by trafficking

<sup>&</sup>lt;sup>46</sup> For example, see Amanda Bodker and others, "Card-not-present fraud: using crime scripts to inform crime prevention initiatives", *Security Journal*, vol. 36, No. 4 (December 2022); Claire Seungeun Lee, "A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea", *Crime, Law and Social Change*, vol. 74, No. 2 (September 2020); and Levi, "Organized fraud and organizing frauds".

<sup>&</sup>lt;sup>47</sup> For example, see Rutger Leukfeldt and Jurjen Jansen, "Cyber criminal networks and money mules: an analysis of low-tech and high-tech fraud attacks in the Netherlands", *International Journal of Cyber Criminology*, vol. 9, No. 2 (December 2015); Michael Skidmore and Beth Aitkenhead, "Understanding the characteristics of serious fraud offending in the UK" (London, The Police Foundation, 2023); Olayinka Akanle, J.O. Adesina and E.P. Akarah, "Towards human dignity and the internet: the cybercrime (*yahoo yahoo*) phenomenon in Nigeria", *African Journal of Science, Technology, Innovation and Development*, vol. 8, No. 2 (2016); and Tiggey May and Bina Bhardwa, *Organised Crime Groups Involved in Fraud*, Crime Prevention and Security Management Series (London, Palgrave Macmillan, 2018).

<sup>&</sup>lt;sup>48</sup> For example, see May and Bhardwa, Organised Crime Groups Involved in Fraud; Usman Adekunle Ojedokun and Ayomide Augustine Ilori, "Tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria", International Journal of Criminal Justice, vol. 3 (2021); Jienan Liu and others, "Understanding, measuring, and detecting modern technical support scams", in 8th Institute of Electrical and Electronics Engineers (IEEE) European Symposium on Security and Privacy, paper presented at the Symposium held in Delft, Kingdom of the Netherlands, from 3 to 7 July 2023; and Vaclav Jirovsky and others, "Cybercrime and organized crime", in ARES 18: Proceedings of the 13th International Conference on Availability, Reliability and Security, art. No. 61 (Hamburg, Germany, 2018).

<sup>&</sup>lt;sup>49</sup> Skidmore and Airkenhead, "Understanding the characteristics of serious fraud offending"; and Neal Shover, Glenn S. Coffey and Clinton Robert Sanders, "Dialing for dollars: opportunities, justifications, and telemarketing fraud", *Qualitative Sociology*, vol. 27, No. 1 (March 2004).

<sup>&</sup>lt;sup>50</sup> This distinguishes organized criminal groups that adopt "associational criminal structures" from those that adopt "entrepreneurial criminal structures" (Klaus von Lampe, *Organized Crime: Analyzing Illegal Activities, Criminal Structures, and Extra-legal Governance* (Los Angeles, California, Sage Publications, 2016)).

<sup>&</sup>lt;sup>51</sup>One illustrative example is the Black Axe Confraternity, a long-standing organized criminal group that emanates from Nigeria but has members located in various countries. They are involved in multiple forms of organized crime that include trafficking in persons and drug trafficking, as well as romance fraud and other cybercrimes. See Nate Allen, Matthew La Lime and Tomsin Sammer-Nlar, *The Downsides of Digital Revolution: Confronting Africa's Evolving Cyber Threats* (Geneva, Global Initiative against Transnational Organized Crime, 2022); and Kim-Kwang Raymond Choo, "Organized crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, No. 3 (September 2008).

<sup>&</sup>lt;sup>52</sup>In addition to being formed on the basis of social bonds, some groups can adopt "quasi-governmental criminal structures" by imposing governance structures and control over crime and criminals within a locality and, in some cases, corrupting public officials (von Lampe, Organized Crime: Analyzing Illegal Activities).

<sup>53</sup> Mortley, "A crime of opportunity"; and Akanle, Adesina and Akarah, "Towards human dignity and the internet".

victims who are tricked or coerced into perpetrating fraud.<sup>54</sup> In some instances, the profits from fraud can be used by the organized criminal groups to fund other serious criminal activities. There are some examples in which fraud features in the nexus between organized crime and terrorism, whereby fraud provides the means to finance the activities of terrorist organizations.<sup>55</sup>

Many organized criminal groups involved in fraud are formed for the singular purpose of perpetrating fraud to make an illicit profit. The relationships between co-offenders can be rooted in close social bonds, <sup>56</sup> but it is also common for relationships to emerge from markets in which knowledge and resources are bought and sold. <sup>57</sup> This fosters fluid collaborative arrangements, with co-offenders coalescing around "project" crimes that are time-limited. The relationships between group members can be transactional or short-lived, or they may last only as long as the fraudulent scheme is successful. <sup>58</sup> Some organized criminal groups mimic a legitimate workforce structure that occupies office space, with co-offenders employed as salaried members of staff or contracted to provide a service. <sup>59</sup> However, co-offending in the context of cyberfraud can also be rooted in relationships established online. In addition to creating new criminal opportunities to perpetrate fraud, <sup>60</sup> the Internet has lowered the barriers to forming relationships with new prospective co-offenders: it has created more accessible environments in which new and anonymous offenders can quickly establish trust and draw from the criminal capital available in online networks. <sup>61</sup> This is exemplified by the crime-as-a-service model, <sup>62</sup> in which criminals engage in short-term online exchanges with others on the Internet who can supply the technical resources to successfully perpetrate fraud. <sup>63</sup> Some organized criminal groups engaged in

<sup>&</sup>lt;sup>54</sup> Office of the United Nations High Commissioner for Human Rights (OHCHR), "Online scam operations and trafficking into forced criminality in Southeast Asia: recommendations for a human rights response" (Bangkok, Regional Office for South-East Asia, 2023); UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia: Policy Report (Bangkok, 2023); and Global Report on Trafficking in Persons 2022 (United Nations publication, 2022), p. 102.

<sup>55</sup> Nicholas Ryder and Samantha Bourton, "To exchange or not to exchange – that is the question: a critical analysis of the use of financial intelligence and the exchange of information in the United Kingdom", *Journal of Business Law*, vol. 3 (2024); and Frank S. Perri and Richard G. Brody, "The dark triad: organized crime, terror and fraud", *Journal of Money Laundering Control*, vol. 14, No. 1 (2011).

<sup>&</sup>lt;sup>56</sup> Eric Rutger Leukfeldt, "Cybercrime and social ties: phishing in Amsterdam", *Trends in Organized Crime*, vol. 17, No. 4 (December 2014); Jonathan Lusthaus, *Industry of Anonymity: Inside the Business of Cybercrime* (Cambridge, Massachusetts, Harvard University Press, 2018); and Joshua Oyeniyi Aransiola and Suraj Olalekan Asindemade, "Understanding cybercrime perpetrators and the strategies they employ in Nigeria", *Cyberpsychology, Behavior, and Social Networking*, vol. 14, No. 12 (December 2011).

<sup>&</sup>lt;sup>57</sup> Richet, "How cybercriminal communities grow and change"; Lilian Ablon, Martin C. Libicki and Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (Santa Monica, California, RAND Corporation, 2014); and Michael Yip, Nigel Shadbolt and Craig Webber, "Structural analysis of online criminal social networks", in 2012 IEEE International Conference on Intelligence and Security Informatics, Daniel Zeng and others, eds. (2012).

<sup>&</sup>lt;sup>58</sup> Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>59</sup>Liu and others, "Understanding, measuring, and detecting"; Shover, Coffey and Sanders, "Dialing for dollars"; and May and Bhardwa, Organised Crime Groups Involved in Fraud.

<sup>&</sup>lt;sup>60</sup> Jay S. Albanese, "Fraud: the characteristic crime of the twenty-first century", *Trends in Organized Crime*, vol. 8, No. 4 (June 2005); Mark Button and Cassandra Cross, *Cyber Frauds, Scams and Their Victims* (Abingdon, Oxon, United Kingdom and New York, Routledge, 2017); and Robert B. Fried, "Cyber scam artists: a new kind of con" (2001).

<sup>&</sup>lt;sup>61</sup> Geralda Odinot and others, Organised Cybercrime in the Netherlands: Empirical Findings and Implications for Law Enforcement (The Hague, Research and Data Centre, Ministry of Security and Justice, 2017); Ablon, Libicki and Golay, Markets for Cybercrime Tools and Stolen Data; and Michael Yip, Craig Webber and Nigel Shadbolt, "Trust among cybercriminals? Carding forums, uncertainty and implications for policing", Policing and Society: An International Journal of Research and Policy, vol. 23, No. 4 (2013).

<sup>62</sup> Online marketplaces, custom websites and forums can operate to their own organizational structure: the administrators, who manage the sites, the moderators, who regulate behaviour on the site, the sellers, who supply the products, services and expertise, and the buyers, who make purchases and engage in information exchange. In this context, technical skills and resources are prized over physical presence and power (Yip, Webber and Shadbolt, "Trust among cybercriminals?"; Ildiko Pete and others, "A social network analysis and comparison of six dark web forums", in 5th IEEE European Symposium on Security and Privacy Workshops (2020); and Choo and Smith, "Criminal exploitation of online systems").

<sup>&</sup>lt;sup>63</sup> See also Ugur Akyazi, Michael van Eeten and Carlos H. Gañán, "Measuring cybercrime as a service (CaaS) offerings in a cybercrime forum" (Delft, Kingdom of the Netherlands, Delft University of Technology, 2021); and Jungkook An and Hee-Woong Kim, "A data analytics approach to the cybercrime underground economy", *IEEE Access*, vol. 6 (2018).

cyberfraud are formed from relationships that exist entirely online (e.g. online forums),<sup>64</sup> others are formed offline and some incorporate both offline and online co-offenders.<sup>65</sup>

There are organized criminal groups engaged in white-collar or corporate fraud that emerge from within legitimate business organizations. <sup>66</sup> The abuse of a legitimate role to gain illegal profit may serve the interests of specific staff members within the organization or may be intended to benefit the whole organization. <sup>67</sup> Organized criminal groups may emerge from the structures that already exist in the business for conducting its legitimate business activity, such as the roles and hierarchy internal to the organization or relationships between different businesses. Examples include the involvement of senior staff members and subordinates within the business, the use of key professionals such as accountants or lawyers, and co-offending by different organizations in a sector, such as in cases of insider trading. <sup>68</sup>

There are overlaps between the different types of organized criminal groups that are engaged in fraud, in part due to the fluidity of co-offending arrangements in certain online and business settings.<sup>69</sup> For example, cyber-entrepreneurs, or finance specialists, supply specialist knowledge and resources that are highly valued by multiple organized criminal groups seeking to augment their capabilities.<sup>70</sup> The fluid and ephemeral nature of the co-offending that characterizes much of organized fraud means that many organized criminal groups involved in it do not display the traditional structures observed in groups involved in other forms of organized crime.<sup>71</sup> As a result, there are challenges to identifying, assessing and delivering effective responses to groups that are loosely structured and transient. For example, in online criminal markets (or ecosystems), it can be difficult to know where one organized criminal group ends and the next begins.<sup>72</sup> Nevertheless, it is important to be able to recognize organized criminal groups that adopt these diverse structures to ensure that the most impactful perpetrators are targeted.

Importantly, not all groups of co-offenders who perpetrate fraud constitute an organized criminal group in accordance with the Organized Crime Convention. This is because the perpetration of serious fraud is also a key defining principle of organized crime. The key characteristics of serious crime in the context of fraud offences will be discussed in the next section.

<sup>&</sup>lt;sup>64</sup> Melvin R.J. Soudijn and Birgit C.H.T. Zegers, "Cybercrime and virtual offender convergence settings", *Trends in Organized Crime*, vol. 15, Nos. 2 and 3 (September 2012).

<sup>&</sup>lt;sup>65</sup> Leukfeldt, Lavorgna and Kleemans, "Organised cybercrime or cybercrime that is organised?"; and E. Rutger Leukfeldt, Edward R. Kleemans and Wouter P. Stol, "Origin, growth and criminal capabilities of cybercriminal networks: an international empirical analysis", *Crime Law and Social Change*, vol. 67, No. 1 (February 2017).

<sup>&</sup>lt;sup>66</sup> Alan Wright, *Organised Crime* (Cullompton, United Kingdom, Willan Publishing, 2006); Gary Slapper and Steve Tombs, *Corporate Crime* (Harlow, United Kingdom, Pearson, 1999); Albanese, "Organized crime as financial crime"; and Michael Levi and Mike Maguire, "Financial and organised crime in Europe: converging paradigms of control?", in *Universalis. Liber amicorum Cyrille Fijnaut*, Toine Spapens, Marc Groenhuijsen and Tijs Kooijmans, eds. (Antwerp, Belgium, Intersentia, 2011).

<sup>&</sup>lt;sup>67</sup> For example, corporate criminal groups were identified as a key manifestation of organized crime in the context of the illegal wildlife trade: corporate criminal acts could be the product of deliberate decision-making or culpable negligence within a legitimate organization (Tanya Wyatt, Daan van Uhm and Angus Nurse, "Differentiating criminal networks in the illegal wildlife trade: organized, corporate and disorganized crime", *Trends in Organized Crime*, vol. 23, No. 4 (December 2020). See also Reurink, *Financial Fraud*).

<sup>&</sup>lt;sup>68</sup> Levi, "Organized fraud and organizing frauds"; and Ruben Herrera and others, "The manipulation of Euribor: an analysis with machine learning classification techniques", *Technological Forecasting and Social Change*, vol. 176, art. No. 121466 (March 2022).

<sup>&</sup>lt;sup>69</sup> Leukfeldt, Kleemans and Stol, "Origin, growth and criminal capabilities of cybercriminal networks"; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>70</sup> Button and Cross, Cyber Frauds, Scams and Their Victims.

<sup>&</sup>lt;sup>71</sup> Di Nicola, "Towards digital organized crime"; Anita Lavorgna and Anna Sergi, "Serious, therefore organised? A critique of the emerging 'cyber-organised crime' rhetoric in the United Kingdom", *International Journal of Cyber Criminology*, vol. 10, No. 2 (July/December 2016); David S. Wall, "Dis-organised crime: towards a distributed model of the organisation of cybercrime", *European Review of Organised Crime*, vol. 2, No. 2 (2015); Leukfeldt, Lavorgna and Kleemans, "Organised cybercrime or cybercrime that is organised?"; and Levi, "Organized fraud and organizing frauds".

<sup>&</sup>lt;sup>72</sup> For example, see Erika Kraemer-Mbula, Puay Tang and Howard Rush, "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change*, vol. 80, No. 3 (March 2013).

#### CASE STUDY: TECHNICAL SUPPORT SCAM



The perpetrators of the technical support scam developed fraudulent websites to mimic legitimate technical support services (e.g. security software or the fixing of printers), which were advertised using mainstream web search engines. Those who visited the website were prompted to call a telephone number, whereupon the call handler would persuade the victim to pay significant amounts of money for a fabricated or unnecessary service. The criminals involved in these scams operated as part of a vibrant underground economy, in which organized criminal groups bought and sold specialist services in chat groups that operated on mainstream social media platforms. Criminals operated as discrete sub-businesses that delivered specific functions in the commission of the technical support scam. These functions included the call centre operators who handled the victims' calls, groups that specialized in money-laundering and sold their services to the call centres and the persons who built and promoted the websites and sold and redirected the victims' calls to the call centre operators. While much of the collaboration between the different sub-businesses was established online, there was a concentration of offenders in India. Many of the call centres operated from office spaces located in large cities across India, and job advertisements for call agents were regularly posted in online forums, giving details of the salary and employment benefits.

Source: Jienan Liu and others, "Understanding, measuring, and detecting modern technical support scams", in 8th Institute of Electrical and Electronics Engineers (IEEE) European Symposium on Security and Privacy, paper presented at the Symposium held in Delft, Kingdom of the Netherlands, from 3 to 7 July 2023.

#### CASE STUDY: CONSUMER FRAUD



An offender set up multiple fake online shops that were made to look credible by appearing similar to other mainstream online retailers, although none of the products advertised on the site existed. The websites were heavily advertised on a mainstream Internet search engine and price comparison websites and in newspapers. Each customer who placed an order would receive an automated order confirmation, receipt and a payment request asking for a wire transfer. The offender searched for an accomplice to help supply the bank accounts to receive the money. He found a co-offender on a darknet forum. This co-offender advised him on how to launder the criminal proceeds and avoid detection by the authorities. He helped to recruit multiple money mules with foreign bank accounts who agreed to receive the payments from customers, taking 15 per cent for themselves and then forwarding the remainder to the two main offenders, who would share the remainder of the criminal profits. The group was able to steal over €280,000 from customers.

Source: Munich District Court, Judgment, 7 June 2017 (LG München, Urteil vom 07.06.2017, 19 KLs 30 Js 18/15), available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

## CASE STUDY: AUCTION FRAUD INVOLVING AN OFFLINE-ONLINE HYBRID ORGANIZED CRIMINAL GROUP



The offenders perpetrated online fraud in which non-existent items were advertised to consumers in the United States of America on mainstream auction sites. The members of the group who planned and prepared the fraudulent scheme were all located in the same town in Romania. They asked consumers to make payments using prepaid debit cards. These payments were collected by other associates and third party money-launderers located in the United States. Once the victims' payments had been collected, the United States-based offenders converted the money into bitcoin, which was transferred to the group in Romania. Bitcoin exchanges were used to convert the money into the local currency, which included an exchange operated by a Bulgarian national who was complicit in facilitating the money-laundering process.

Source: United States of America v. Andre-Catalin Stoica et al., available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

#### Serious crime in the context of fraud

The concept of serious crime is a central one in the definition of the scope of application of the Organized Crime Convention. For the Convention to be applicable, the crime committed by the organized criminal group has to meet the criteria defined (including transnationality and the involvement of an organized criminal group) and be punishable by a maximum deprivation of liberty of at least four years in national legislation. Therefore, the use of the notion of serious crime with reference to the national law of States provides sufficient flexibility for the Convention to be applied to a broad range of manifestations of transnational organized crime, including fraud.

A "serious crime" is defined in article 2 (b) of the Convention as "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty". Article 3, paragraph 2, of the Convention sets out the criteria for determining when an offence will be considered transnational in nature, for the purpose of application of the Convention.

Internationally, existing legal systems are equivocal on the seriousness of fraud. The specific aggravating factors that can individually or accumulatively increase the penalties for convicted fraudsters, and the maximum penalty that can be applied in a fraud case, vary across different legal jurisdictions (see chap. V below). This is reflected in the penalties given to fraud offenders: for example, long custodial sentences handed down to white-collar offenders who defraud institutions have been shown to be low in number, despite the prevalence of this offence and the high profits for offenders.<sup>73</sup> Furthermore, some of the most sophisticated types of fraud brush against the grey margins that separate legitimate from illegitimate practices, and criminal law (and its enforcement) can be substituted for civil laws enforced by regulatory bodies in the wider public sector.<sup>74</sup> The uneven treatment of fraud in law fosters ambiguity in identifying "serious" fraud and fraudsters.

<sup>&</sup>lt;sup>73</sup>Michael Levi, "Hitting the suite spot: sentencing frauds", *Journal of Financial Crime*, vol. 17, No. 1 (2010); and Lisa Marriott, "White-collar crime: the privileging of serious financial fraud in New Zealand", *Social and Legal Studies*, vol. 29, No. 4 (August 2020).

<sup>74</sup> Button and Cross, Cyber Frauds, Scams and Their Victims.

There are two primary dimensions of seriousness to consider:75

- The harm that can be attributed to the fraud, in terms of either the identifiable victim or victim group or the wider impact it has on legitimate institutions<sup>76</sup>
- The moral culpability of the perpetrator(s), meaning the extent to which certain behaviours violate accepted moral standards in society<sup>77</sup>

The various victims, victim experiences, offending behaviours and methods mean that, as a category of crime, fraud incorporates criminality that is highly diverse in relation to the gravity of the harms that are caused and the moral wrongfulness of the offending behaviours. Multiple factors might be perceived to aggravate a fraud offence and thereby render it more serious. Such factors include the financial impact on and harm to the victim but also specific offending behaviours such as targeting vulnerable victims, having repeat contact with the same victim to engage in more complex or insidious methods (e.g. grooming), abusing a position of trust or authority to defraud victims and targeting a large number of victims.<sup>78</sup>

There is a need to consider the evidence on the characteristics of fraud offending that can be used to determine whether certain fraud offences ought to be treated as serious crime in terms of sentencing and wider criminal justice policy. Those characteristics are set out in the sections below.

#### Financial losses and impact

Fraud is an acquisitive crime, and the value of monies that are stolen (or were intended to be stolen) inform the assessments of its seriousness. This can be viewed as the aggregate intended or actual losses attributable to offenders who defraud multiple victims. Different offending behaviours can lead to distinct patterns in defrauding and financial loss. Some fraudulent schemes affect a relatively small number of victims who are defrauded of significant amounts of money, whereas others defraud a larger number of victims of smaller amounts of money. Assessments of losses to victims may also factor in who the victims are (e.g. an individual or corporation), the proportion of a victim's wealth lost to the fraud and other wider collateral damage caused. Fraud can undermine legitimate sectors, imposing costs beyond the direct losses to the organization that is targeted.

<sup>&</sup>lt;sup>75</sup> An Adriaenssen and others, "Public perceptions of the seriousness of crime: weighing the harm and the wrong", *European Journal of Criminology*, vol. 17, No. 2 (March 2020); Jonas Visschers and Letizia Paoli, "A comparison of public and police perceptions of the seriousness of crime", *European Journal on Criminal Policy and Research* (2024); and Victoria A. Greenfield and Letizia Paoli, "A framework to assess the harms of crimes", *The British Journal of Criminology*, vol. 53, No. 5 (September 2013).

<sup>&</sup>lt;sup>76</sup>Tom Sorell, "The scope of serious crime and preventive justice", Criminal Justice Ethics, vol. 35, No. 3 (2016).

<sup>&</sup>lt;sup>77</sup> For example, regardless of the harm that is experienced, burglary might be construed as a greater violation of moral norms than theft due to the attack on the integrity of the victim's home.

<sup>&</sup>lt;sup>78</sup> Button and others, "Online frauds".

<sup>79</sup> For example, see Skidmore, Protecting People's Pensions.

<sup>&</sup>lt;sup>80</sup> For example, see Marguerite DeLiema and Paul Witt, *Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam*, Working Paper, No. 2021-434 (Ann Arbor, University of Michigan, Michigan Retirement and Disability Research Center, 2021).

<sup>&</sup>lt;sup>81</sup> Michael Levi, "Organized fraud", in *The Oxford Handbook of Organized Crime*, Letizia Paoli, ed. (Oxford, Oxford University Press, 2014); and Xin Qingquan, Jing Zhou and Fang Hu, "The economic consequences of financial fraud: evidence from the product market in China", *China Journal of Accounting Studies*, vol. 6, No. 1 (2018).

<sup>&</sup>lt;sup>82</sup> For example, so-called crash-for-cash fraud against the car insurance sector can raise insurance premiums for the public (David S. Wall, Yulia Chistyakova and Stefano Bonino, "Crash-for-cash and VAT carousels: organised crime infiltration in the United Kingdom", in *Organised Crime in European Businesses*, Ernesto Savona, Michele Riccardi and Giulia Berlusconi, eds. (London, Routledge, 2016)).

#### Harm to victims

Fraud mostly occurs behind closed doors and rarely involves publicly visible or visceral crimes such as serious violence that are a conventional focus for law enforcement agencies. Furthermore, criminal justice sentencing policies can have a singular focus on financial loss, without considering the human impact of fraud. Research has identified victims who experience a considerable detrimental effect on their psychological and emotional well-being and physical health; in extreme cases, victims have taken their own lives as a consequence of fraud.<sup>83</sup> Victim responses are highly subjective and can be determined by their personal circumstances and the particularities of the fraud methodology.<sup>84</sup> The wide-ranging and subjective nature of victim experiences means that there are challenges to identifying vulnerability and harm from among the high volume of fraud victims.<sup>85</sup>

#### Fraudster culpability

Culpability reflects in part the level of criminal intent that is displayed by a perpetrator, such as the extent of planning and premeditation and evidence of repeat offending. The complex processes for perpetrating fraud commonly entail stages of planning and preparation, and some offenders continuously innovate new methods to exploit the range of available criminal opportunities. <sup>86</sup> The growth in ICTs has "industrialized" fraud offending, providing greater scope for criminals to perpetrate fraud on an unprecedented scale, at speed and at low cost. <sup>87</sup> Criminals can harness technology to target many victims simultaneously, in some cases by means of automation. <sup>88</sup> Furthermore, ICTs are globalized as a default and, in some cases, there is little practical difference between perpetrating local or transnational fraud. <sup>89</sup> In this context, the line separating serious from non-serious criminals can be difficult to draw.

The specific methods employed for targeting and defrauding victims can determine the perceived gravity of the fraudster's actions. This includes targeting, sometimes repeatedly, persons who are in some way disadvantaged, such as victims who are perceived as vulnerable (e.g. persons with a disability). The abuse of a position of power or trust is also considered an aggravating factor in fraud offences in some legal jurisdictions. Lastly, the involvement of an organized criminal group can itself multiply the adverse effects of fraud and signal greater criminal intent and culpability. An organized criminal group that maintains a criminal "institution" with a ready supply of co-offenders for perpetrating fraud on

<sup>&</sup>lt;sup>83</sup> For example, see Button, Lewis and Tapley, "Not a victimless crime"; Cassandra Cross, "(Mis)understanding the impact of online fraud: implications for victim assistance schemes", *Victims and Offenders*, vol. 13, No. 6 (2018); Raoul Notté and others, "Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands", *International Review of Victimology*, vol. 27, No. 3 (September 2021); and Encarnación Sarriá and others, "Financial fraud, mental health, and quality of life: a study on the population of the city of Madrid, Spain", *International Journal of Environmental Research and Public Health*, vol. 16, No. 18 (September 2019).

<sup>&</sup>lt;sup>84</sup> For example, romance fraud has been shown to cause significant emotional distress to victims (Tom Buchanan and Monica T. Whitty, "The online dating romance scam: causes and consequences of victimhood", *Psychology, Crime and Law*, vol. 20, No. 3 (2014). See also Katelyn A. Golladay and Jamie A. Snyder, "Financial fraud victimization: an examination of distress and financial complications", *Journal of Financial Crime*, vol. 30, No. 6 (2023)).

<sup>&</sup>lt;sup>85</sup> Michael Skidmore, Janice Goldstraw-White and Martin Gil, "Vulnerability as a driver of the police response to fraud", *Journal of Criminological Research, Policy and Practice*, vol. 6, No. 1 (2020); and Sara Correia, "Cybercrime victims: victim policy through a vulnerability lens", Social Science Research Network Working Paper (2021). In the United Kingdom, there is an increasing focus on identifying vulnerable victims, particularly those at risk of being targeted repeatedly.

<sup>&</sup>lt;sup>86</sup> For example, see Kraemer-Mbula, Tang and Rush, "The cybercrime ecosystem"; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>87</sup> Button and Cross, *Cyber Frauds, Scams and Their Victims*; and Michael Levi and others, *The Implications of Economic Cybercrime for Policing*, Research Report (London, City of London Corporation, 2015).

<sup>88</sup> Wall, "Dis-organised crime"; and van der Wagen and Pieters, "From cybercrime to cyborg crime".

<sup>89</sup> Levi and others, The Implications of Economic Cybercrime for Policing.

<sup>&</sup>lt;sup>90</sup> Research into the views of the public in the United Kingdom showed that insidious methods such as financial grooming were perceived to represent more serious types of fraud (see Jane Kerr and others, *Research on Sentencing Online Fraud Offences* (London, Sentencing Council, 2013)).

<sup>&</sup>lt;sup>91</sup> Marriott, "White-collar crime"; see also chapter V of the present issue paper.

a continuous basis (as well as other ancillary crimes, such as illicit hacking and money-laundering),<sup>92</sup> can engage in criminality that is considered more serious.<sup>93</sup> Furthermore, the criminality can become even more serious when the group is able to challenge or undermine the authority and systems of the State and legitimate sectors (for example, by means of corruption).<sup>94</sup>

Sentencing frameworks in the criminal justice system provide important guidance to law enforcement agencies in deciding where to target available resources. The increased scope of complexity of fraud offending, particularly that enabled by technology, creates challenges in the identification of serious fraud, but robust frameworks are needed to target the most egregious fraud cases. The precise dimensions of organized fraud in each Member State will need to be taken into account in policy decisions on resourcing law enforcement and wider crime prevention strategies for tackling fraud. Historically, however, fraud committed by organized criminal groups has not been afforded the same levels of priority given to other manifestations of organized crime, 95 and organized fraud has often been perceived as a supplementary activity of organized criminal groups involved in other, more serious crimes (e.g. drug trafficking). 96

## Intersectionality

A key concept in understanding people's experiences of organized fraud is intersectionality. Intersectionality constitutes a framework for analysing how power and identity intersect to influence social relations and individual experiences. It emphasizes that the experiences of men, women and gender-diverse individuals interact with their class, race, age, ethnicity and sexual and other identities, thereby shaping the ways in which people are perceived in society. In the context of organized fraud, an intersectional analysis is a useful tool to understand the different trends and drivers for participating in and becoming a victim of organized fraud. This is not to say that certain identity characteristics lead to a person being inherently vulnerable to organized fraud but that, due to structural, historical and contextual factors, a person's privilege and power can be affected under specific circumstances, leading to differentiated experiences of organized fraud. The case study below highlights how organized criminal groups may take advantage of the social and historical exclusion faced by persons with disabilities to carry out organized fraud.

<sup>&</sup>lt;sup>92</sup> Leukfeldt and Jansen, "Cyber criminal networks and money mules"; Jonathan Lusthaus and others, "Cybercriminal networks in the United Kingdom and beyond: network structure, criminal cooperation and external interactions", *Trends in Organized Crime* (2023); David S. Wall, "Digital realism and the governance of spam as cybercrime", *European Journal on Criminal Policy and Research*, vol. 10, No. 4 (December 2004); and Michael Yip, Nigel Shadbolt and Craig Webber, "Why forums? An empirical analysis into the facilitating factors of carding forums", in *Proceedings of the 3rd Annual ACM Web Science Conference* (Paris, 2013).

<sup>93</sup> Sorell, "The scope of serious crime".

<sup>&</sup>lt;sup>94</sup> For example, organized criminal groups operating across South-East Asia engage in systemic criminality and generate profits from fraud estimated to be worth billions of dollars. These groups have a long-standing involvement in various forms of organized crime, and the capacity to perpetrate fraud on this scale is linked to parallel developments in underground banking and money-laundering, specifically casinos. The casinos can facilitate money-laundering but also provide a front and a facility to employ a large workforce to co-offend from within scam compounds. Furthermore, some groups purposefully operate from within countries where governance and the rule of law are weak and public officials are susceptible to corruption (see OHCHR, "Online scam operations and trafficking into forced criminality in Southeast Asia"; and UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat, Technical Policy Brief (Bangkok, 2024)).

<sup>&</sup>lt;sup>95</sup> Alan Doig and Michael Levi, "A case of arrested development? Delivering the UK National Fraud Strategy within competing policing policy priorities", *Public Money and Management*, vol. 33, No. 2 (2013); and Cassandra Cross and Dom Blackshaw, "Improving the police response to online fraud", *Policing*, vol. 9, No. 2 (June 2015).

<sup>&</sup>lt;sup>96</sup>Levi, "Organized fraud", in The Oxford Handbook of Organized Crime.

#### CASE STUDY: CONSUMER PRODUCTS AND SERVICES AND INVESTMENT FRAUD



In the United Kingdom, an individual suffering from a progressive neurological condition was groomed over a number of years by a small, family-based organized criminal group. The principal offender was ostensibly a tradesman who met the victim when looking for potential customers. The group completed and overcharged for a multitude of substandard repairs and maintenance work on the victim's house. Furthermore, they persuaded him to hand over £240,000, which included money for a purported investment opportunity. The victim did not recognize that he was a victim because the perpetrators had gone to considerable lengths to befriend him and, accordingly, he thought he was helping people who were his friends. The fraud was eventually reported by his carer, and enforcement officers had to explain carefully how and why he had been a victim of fraud. This example illustrates how some organized criminal groups target persons with disabilities owing to the likelihood of persons with disabilities experiencing social isolation and not having adequate access to social support.

Source: Coretta Phillips, "From 'rogue traders' to organized crime groups: doorstep fraud of older adults", The British Journal of Criminology, vol. 57, No. 3 (May 2017).

It is important to recognize that there are no specific identity characteristics that make a person more vulnerable to organized fraud. This is due to its many manifestations and typologies. For example, an individual with a high income may be targeted for investment fraud, whereas an individual in a lower socioeconomic bracket may be targeted for employment fraud. For this reason, and to be able to develop effective preventive measures, it is important to collect intersectional, gender-disaggregated data and to carry out analysis to identify why certain populations may be targeted for different types of fraud.



## CHAPTER II

## Categories of organized fraud

Fraud offending is highly diverse, in the methods employed, the entities targeted and the impact on victims and wider systems. The present issue paper is focused on fraud that is targeted at individual members of the public or private institutions for the purposes of obtaining a financial or other material benefit.

The categories in the typology are arranged according to the overarching and predominant narratives or ruses that are presented to fraud victims; <sup>97</sup> for example, the marketing of an employment opportunity in employment fraud. However, the category of fraud against businesses and organizations is also included to encompass the range of fraud against such entities, <sup>98</sup> including the abuse of systems by perpetrators who are internal or external to the organization. <sup>99</sup> In this way, the categories of fraud are primarily arranged according to a victim-based perspective of fraud, not the underlying processes in the commission of the crime, such as the processes for stealing personal data or the modes of marketing or other mass communication.

The key categories that will be described in the following sections of the issue paper are:



<sup>97</sup> See, for example, Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>&</sup>lt;sup>98</sup> This category was included to ensure that businesses and organizations are recognized as a key victim group. Other categories, such as consumer products and services fraud and identity fraud, can also lead to financial losses for businesses and organizations.

<sup>&</sup>lt;sup>99</sup> See the introduction to the present issue paper for a more detailed discussion on developing the typology.

In arranging categories by the various narratives or ruses presented to victims, this typology brings to light other broad distinctions in the techniques used to manipulate victims into parting with their money. Key overarching distinctions include the use of sales and enticements in consumer products and services, employment and consumer investment fraud; the fear and authority that characterize many types of fraud in which a perpetrator impersonates a trusted individual or organization; the manipulation of commercial and financial information and systems in identity fraud; and the financial grooming and exploitation in relationship and trust fraud. Other elements of the interaction with offenders that may affect the experience of victims (e.g. the mode of contact or the time period over which they are targeted) will be discussed where relevant under each category.

The categories described in the present section are not intended to be exhaustive because of the near boundless range of methodologies that can be employed by offenders, who continuously adapt to new socioeconomic contexts, systems and technology. Each overarching category is supplemented by prominent subcategories that are described in each section. Not all fraud categories are perpetrated exclusively by organized criminal groups, but the discussion will be focused on organized fraud.

The line separating fraud from non-criminal behaviours can be fine. For example, not all instances of a product or service falling short of what is marketed and sold to a consumer will meet the legal criteria for fraud; in accordance with the discussion in chapter I, it will depend on whether there was criminal intent to deceive. In the context of organized crime, the criminal intent is evident in many key actions, such as the planning and preparatory stages for implementing a deception and using the deceptive technique to target multiple victims. All categories and cases discussed in the present section are assumed to fulfil the definition of fraud as discussed in chapter I: those who commit them are criminally liable due to a deliberate use of deception for the purposes of obtaining a financial or other material benefit.

## Consumer products and services fraud

Consumer products and services fraud represents a prevalent type of fraud, with large numbers of members of the public reporting being defrauded, targeted or exposed to communications selling fraudulent products or services.<sup>100</sup> Oftentimes, fraudsters market in-demand products or offer products and services at a cost below that on the legitimate market. Consumer products and services fraud involves the sale of products or services that are either non-existent or significantly differ from what is advertised (including counterfeit goods sold as genuine).<sup>101</sup> Non-delivery fraud involves advertising and taking payment for products or services that are entirely fictitious or that the fraudster has no intention to supply.<sup>102</sup> The mis-selling of products and services involves fraudsters who misrepresent the goods or services that they are supplying. There can be challenges in confirming fraud when the product or service is received but considered to have been misrepresented, and judgment is required as to how and to what extent the product or service deviates from what was marketed or sold.<sup>103</sup> Some fraudsters target advertisements at groups considered most susceptible to a specific scheme.<sup>104</sup> Sometimes, fraudsters

<sup>&</sup>lt;sup>100</sup> For example, non-payment or non-delivery fraud is one of the most commonly reported cybercrimes in the United States (United States, Federal Bureau of Investigation, "Internet crime report 2023" (2023); see also European Commission, "Survey on 'scams and fraud experienced by consumers': final report" (Brussels, 2020)).

<sup>&</sup>lt;sup>101</sup>Button and Cross, *Cyber Frauds, Scams and Their Victims*; see also *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (United Nations publication, 2010), chap. 8.

<sup>102</sup> United States Federal Bureau of Investigation, "How we can help you: holiday scams", available at http:///www.fbi.gov.

<sup>&</sup>lt;sup>103</sup>In some regions, public sector regulators may be responsible for identifying and responding to fraud. Such regulators include agencies with a remit to protect consumers or regulate professional practices.

<sup>&</sup>lt;sup>104</sup> Keith B. Anderson, "Mass-market consumer fraud: who is most susceptible to becoming a victim?", Working Paper, No. 332 (Washington D.C., Bureau of Economics, Federal Trade Commission, 2016). See also discussion of mass-marketing in chapter IV of the present issue paper.

exploit a victim's lack of financial and technical literacy to sell financial services such as loans, insurance plans or pension products<sup>105</sup> 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 not given a proper explanation of the risks. The fraudsters may also fail to disclose charges, commissions or legal requirements to the victim, which can lead to further losses and penalties.<sup>106</sup>

Products and services that have commonly been featured in consumer products and services fraud include gemstones, pets, event tickets, medical products, food, insurance, clairvoyance or psychic products and services, loans and debt relief.<sup>107</sup> 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. This was exemplified during the coronavirus disease (COVID-19) pandemic, when fake or non-existent medical products were being advertised.<sup>108</sup>

This increase in variety has been facilitated by the growth in online commercial sites, particularly peer-to-peer sales and auction sites, and, increasingly, social media platforms on which all types of products are sold. <sup>109</sup> Products and services are marketed through various media, including fake websites, legitimate shopping and auction sites and spam emails. Other approaches include postal mail, high-volume marketing and sales calls from "boiler rooms", door-to-door sales, mass mailings and unsolicited telephone calls. <sup>110</sup> 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 ("suckers lists"). <sup>111</sup> ICTs have greatly augmented the capacity to market and sell products and services on a global scale and at a 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 also incur a financial loss. Key methodologies include:

- Developing fake websites 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 may manipulate Internet search engines to increase the likelihood that those searching for relevant products or services will land on their website.
- Creating 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 of thousands of listings for high-value items such
  as automobiles on multiple auction sites.<sup>113</sup>

Online consumer fraud does not need to be sophisticated or complex. The abuse of a legitimate sales or auction site can require little more than a single person opening an account on an auction site

<sup>&</sup>lt;sup>105</sup> Investment fraud is included as a separate category below (see also Reurink, *Financial Fraud*).

<sup>106</sup> See, for example, Skidmore, Protecting People's Pensions.

<sup>&</sup>lt;sup>107</sup> Consumer investments are included as a separate category below (see also Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud"; and Mark Button, Chris Lewis and Jacki Tapley, "Fraud typologies and the victims of fraud: literature review" (London, National Fraud Authority, 2009)).

<sup>&</sup>lt;sup>108</sup> United Kingdom, National Crime Agency, "Beware fraud and scams during COVID-19 pandemic fraud", 26 March 2020.

<sup>109</sup> Emma Fletcher, "Social media: a golden goose for scammers", Federal Trade Commission, 6 October 2023.

<sup>&</sup>lt;sup>110</sup> Marguerite DeLiema and Lynn Langton, "Older victims of mass marketing scams: an analysis of data seized from scammers", *Innovation in Aging*, vol. 5, Suppl. No. 1 (2021); Coretta Phillips, "From 'rogue traders' to organized crime groups: doorstep fraud of older adults", *The British Journal of Criminology*, vol. 57, No. 3 (May 2017); and Shover, Coffey and Sanders, "Dialing for dollars".

<sup>&</sup>lt;sup>111</sup>Levi, "Organized fraud", in *The Oxford Handbook of Organized Crime*, p. 460; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>112</sup>The fraudster may pay the technology company or perpetrate "click fraud", whereby bots are used to repeat-click a website link to inflate its search ranking, thereby making the site appear more legitimate.

<sup>&</sup>lt;sup>113</sup> See *United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus*, available from the SHERLOC knowledge management portal.

and posting an advertisement to sell a non-existent product. The role of organized crime is seldom revealed in the exchange with the victim, but rather in understanding the planning and preparation that sit behind it. For example, the production, transportation, sale and distribution of counterfeit products are parts of a complex process that requires the involvement of organized criminal groups with high levels of coordination between co-offenders. <sup>114</sup> In the context of cyberfraud, 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 money. Perpetrators can adopt a variety of methods to receive payments, which 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 and/or using third-party accounts of money mules or accounts opened using stolen or fake identities. Some transnational fraudsters enlist co-offenders within the target country to facilitate money-laundering. <sup>115</sup> Bank accounts are commonly registered to fake, stolen or borrowed identities (e.g. money mules), thereby leaving a limited financial trail.

#### CASE STUDY: ONLINE SHOPPING CONSUMER FRAUD



An independent online sales website advertised high-demand consumer goods to the public in the United Kingdom of Great Britain and Northern Ireland and took thousands of orders from consumers over a period of approximately three months, most of which were not fulfilled. The organized criminal group took the form of a supply chain in which there was an offender overseas who was ostensibly the supplier of the goods, and a distribution centre and online retailer located in separate regions in the United Kingdom. The adoption of a formal supply chain structure created a veneer of legitimacy that could be used to deceive the payment service provider into providing access to its online payment facility for taking customer orders. Most of the products that were sold had never existed, and the money from the purchases was transferred overseas to the fictitious supplier and withdrawn as cash.

Source: Michael Skidmore and Beth Aitkenhead, "Understanding the characteristics of serious fraud offending in the UK" (London, The Police Foundation, 2023).

#### CASE STUDY: ONLINE AUCTION CONSUMER FRAUD



An organized criminal group posted advertisements for high-value products on several online auction websites. The image files that were posted in each advertisement were infected with malware and, when clicked, the malware would then infect the customer's device. The purpose of the malware was to imperceptibly redirect the customers to spoofed web pages that looked identical to those of the legitimate website. The web pages included a live chat function that allowed the buyer to speak to customer service agents who were co-offenders in the group. The customers were asked to pay for items using an "escrow agent", which purportedly held the money for the buyer until they confirmed receipt of the item. However, the money was received into accounts controlled by the offenders and the victims did not receive the ordered items, nor did they receive a refund.

Source: United States of America v. Bogdan Nicolescu, Tiberiu Danet, and Radu Miclaus, available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

<sup>114</sup> Hulme, Disley and Blondes, eds., Mapping the Risk of Serious and Organised Crime.

<sup>115</sup> Christine Conradt, "Online auction fraud and criminological theories: the Adrian Ghighina case", *International Journal of Cyber Criminology*, vol. 6, No. 1 (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 (December 2020).

## **Employment fraud**

Employment fraud involves the mass-marketing of fake or misleading employment or business opportunities to members of the public. This type of fraud entails advertising an opportunity that is either entirely fictional or much less profitable than advertised, and the victims lose money without receiving the promised employment or remuneration. The fraudsters commonly request upfront payments from victims before taking a position or setting up their business; this payment is explained in several different ways, including being for the purchase or leasing of products or equipment needed to establish the business, travel arrangements, the provision of training or the completion of credit score checks. It In other schemes, the fraudsters send advance payments using fraudulent cheques to cover a victim's start-up costs, before claiming that they have made an overpayment and asking victims to transfer back the money. Persons in need of economic opportunities can be particularly vulnerable to this type of fraud.

The substantial growth in online recruitment brings many advantages to legitimate businesses, including the ability to target communications to and assess candidates from a high volume of jobseekers. However, these same advantages can be exploited by fraudsters who use legitimate job sites, online forums and social media to disseminate fraudulent job advertisements to high volumes of jobseekers. It is a considerable challenge for job sites to identify fraudulent advertisements that are posted on their platforms.<sup>119</sup>

Fraudsters exploit the demand for desirable positions, particularly among jobseekers with fewer skills or qualifications, offering working conditions (e.g. work from home or flexible working) or levels of payment normally out of reach. One study in the United States of America found that encountering fraudulent online job advertisements was a regular occurrence for many workers engaged in temporary or insecure work (such as in the gig economy). <sup>120</sup> Economic uncertainty and high unemployment are a breeding ground for employment fraud, whereby the absence of opportunities in the legitimate economy leads to more desperate and risky decision-making among those looking for employment. <sup>121</sup>

Victims are also at risk of being targeted repeatedly because many are asked to provide personal information or identity documents during the fraudulent application process. The primary motivation in some employment fraud is to steal victims' personal data. In other cases, the victims are themselves drawn into facilitating the criminality. For example, fraudulent business opportunities can operate as illegal pyramid schemes in which the profits for the victim come from recruiting others to register with the scheme. Victims who take jobs as couriers can become involved in delivering contraband or stolen goods, and others may become embroiled as money mules to facilitate money-laundering.

 $<sup>^{\</sup>rm 116}\, Beals,$  DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>&</sup>lt;sup>117</sup> 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); and Cassandra Cross and Deanna Grant-Smith, "Recruitment fraud: increased opportunities for exploitation in times of uncertainty?", *Social Alternatives*, vol. 40, No. 4 (2021).

 $<sup>^{\</sup>rm 118}$  Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>&</sup>lt;sup>119</sup> Mohammed A. Sofy, Mohammed H. Khafagy and Rasha M. Badry, "An intelligent Arabic model for recruitment fraud detection using machine learning", *Journal of Advances in Information Technology*, vol. 14, No. 1 (February 2023); and Syed Mahbub and Eric Pardede, "Using contextual features for online recruitment fraud detection", 27th International Conference on Information Systems Development (ISD2018), held in Lund, Sweden, in 2018.

<sup>120</sup> Ravenelle, Janko and Cai Kowalski, "Good jobs, scam jobs".

<sup>121</sup> Cross and Grant-Smith, "Recruitment fraud"; 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).

<sup>122</sup> Sofy, Khafagy and Badry, "An intelligent Arabic model".

<sup>123</sup> Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>124</sup> Ravenelle, Janko and Cai Kowalski, "Good jobs, scam jobs"; and Mohanamerry Vedamanikam, Saralah Devi Mariamdaran Chethiyar and Norruzeyati bt Che Mohd Nasir, "Model for money mule recruitment in Malaysia: awareness perspective", *PEOPLE: International Journal of Social Sciences*, vol. 6, No. 2 (2020).

#### Consumer investment fraud

Consumer investment fraud commonly involves the marketing and sale of securities, including equities and real estate, government or corporate bonds, commodities such as precious metals, and foreign currencies. The perpetrators knowingly mislead investors by providing information that either grossly misrepresents the prospective earnings that can be made from an investment or relate to an investment that does not exist. 127

The commission of these types of fraud can require a keen awareness of the contours of regulation and related controls that govern the markets. 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 for law enforcement and regulators that are required to navigate and produce sufficient and robust evidence of deception and demonstrate that a crime has occurred.<sup>128</sup> Indeed, while unethical, some may employ schemes that cause harm to investors but transpire not to be criminal. Pyramid and Ponzi<sup>129</sup> schemes are common operating models for offenders, whereby the investment scheme is sustained by maintaining a continuous flow of investment from new investors in place of a returns from an actual product or investment that may never have existed.<sup>130</sup> Research has found that gender and age can affect vulnerability to such schemes, with many schemes taking advantage of the gender pay gap and claiming to help women through the provision of economic opportunities and a sense of community.<sup>131</sup>

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.<sup>132</sup> The complexity of the operation is variable and can depend on its intended length. 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.<sup>133</sup>

Victims of investment fraud experience the largest losses when compared with victims of other types of fraud targeting individual members of the public. The victims are deceived and primed with expectations

<sup>125</sup> Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>126</sup> For example, the sale of "penny stock" investments in smaller companies that offer abnormal returns to prospective investors. One common approach is the "pump and dump" scheme, in which a product is actively promoted to artificially inflate (or "pump") demand for an otherwise unknown or little-known stock, before the fraudster then "dumps" their shares to gain for themselves a large profit and other investors consequently experience losses (Bill Hu, Thomas McInish and Li Zeng, "Gambling in penny stocks: the case of stock spam e-mails", *International Journal of Cyber Criminology*, vol. 4, Nos. 1 and 2 (July/December 2010); and Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud").

<sup>&</sup>lt;sup>127</sup> For example, Ponzi schemes market investment opportunities but none of the money is actually invested, and payouts to existing investors are taken from the money received from new investors (Surendranath Rakesh Jory and Mark J. Perry, "Ponzi schemes: a critical analysis", *Journal of Financial Planning* (2011)).

<sup>&</sup>lt;sup>128</sup> Branislav Hock and Mark Button, "Why do people join pyramid schemes?", *Journal of Financial Crime*, vol. 30, No. 5 (2023); and Skidmore, *Protecting People's Pensions*.

<sup>129</sup> Ponzi and Pyramid schemes operate to similar principles, by using money attracted from new investors to repay earlier investors, but pyramid schemes are distinctive because investments are sold as a business opportunity and the investors themselves are rewarded for recruiting new investors (see, for example, Claire Nolasco, Michael Vaughn and Rolando V. del Carmen, "Revisiting the choice model of Ponzi and Pyramid schemes: analysis of case law", *Crime, Law and Social Change*, vol. 60, No. 4 (November 2013)).

<sup>&</sup>lt;sup>130</sup> Hock and Button, "Why do people join pyramid schemes?"; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>131</sup> Li Huang and others, "Gender and age-based investor affinities in a Ponzi scheme", *Humanities and Social Sciences Communications*, vol. 8, art. No. 60 (2021); Delano Law Offices, "Pyramid schemes target females", 1 February 2022; and Taylor Walsh, "Multilevel marketing, an unwinnable lottery: how MLMs illegally target women and minorities using deceptive and predatory recruitment practices and the need for specific and expanded legal protections", *Georgetown Journal of Gender and the Law*, No. XXIV-1 (2002).

<sup>&</sup>lt;sup>132</sup> Shover, Coffey and Sanders, "Dialing for dollars".

<sup>&</sup>lt;sup>133</sup>Levi, "Organized fraud and organizing frauds"; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

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 that it can be years after the initial investment before they realize that they have been defrauded. The particularities of the different schemes and underlying deception vary widely, but may include:

- A complete deception in which the investment service or product never existed
- Knowingly mis-sold worthless or overpriced shares for high-risk investments that are unlikely to yield the promised return
- Market manipulation techniques that artificially inflate the value of investments to unsuspecting investors (see the description of an exit scam below)

The losses and impact on victims may depend on the methodologies employed by the offenders. If, for example, people's pension savings are targeted, it can have a life-changing impact on the individual victim, whereas some cryptocurrency investments can be focused on receiving smaller amounts but from a greater number of victims (see case study below). Once the money has been stolen, the victim may be targeted again by the same or other offenders, who in some cases claim to have an affiliation to a legitimate body that is able to trace and recover the lost money, but the victim is asked to pay an upfront fee (so-called recovery fraud). 134

#### Cryptocurrency investment fraud

The patterns in investment fraud have seen changes in the response to new digital technologies and forms of finance, especially in the decentralized finance sectors that use cryptocurrency and block-chain technology to conduct financial transactions without the need for the intermediary function of a financial institution (e.g. a bank).

Thus, consumer investment fraud appears to be on the increase, in part due to the 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 and, in some cases, harness automated technologies (or bots) to offend repeatedly. In new financial markets, such as the cryptocurrency market, the challenges in regulation create wider gaps to exploit. The perpetrators commonly exploit social media and digital communications applications to market their products, in some cases utilizing images of celebrities or popular culture imagery to persuade victims to invest their money. These new marketing methods have potentially expanded the reach of investment fraud to ensnare a greater volume of more diverse investors, including a large number of investors in their 30s or 40s. 136

The methods that are employed in cryptoinvestment fraud are variable in both technical complexity and novelty, with some techniques, such as the following, transposed from other methods such as market manipulation and financial grooming:

Fraudulent cryptocurrency investment platforms are developed and marketed to persuade victims
to invest in a cryptocurrency. Much like traditional forms of investment fraud, a victim's trust
can be cultivated over time, sometimes with the use of financial grooming techniques (see the

<sup>&</sup>lt;sup>134</sup> For example, see United States, Federal Bureau of Investigation, "Increase in companies falsely claiming an ability to recover funds lost in cryptocurrency investment scams", 11 August 2023.

<sup>&</sup>lt;sup>135</sup> Arianna Trozze, Toby Davies and Bennett Kleinberg, "Of degens and defrauders: using open-source investigative tools to investigate decentralized finance frauds and money laundering", *Journal of Forensic Science International: Digital Investigation*, vol. 46 (September 2023).

<sup>&</sup>lt;sup>136</sup> United States, Department of Justice, Office of Public Affairs, "Justice Department seizes over \$112M in funds linked to cryptocurrency investment schemes", press release, 3 April 2023.

- section on relationship and trust fraud below). In some cases, a fraudulent website or application is developed to show that the victims' investment is performing well, serving to encourage further investment and the recruitment of other investors from within their social network.<sup>137</sup>
- Exit scams, or "rug pulls", involve the creation of a scam token that can be traded with other cryptocurrencies on a decentralized exchange. Once a sufficient number of victims have traded their coins for the token, the offender can withdraw all monies invested, leaving victims with a worthless token. One particular "pump and dump" technique follows a similar logic to a traditional pyramid or Ponzi scheme whereby the fraudsters artificially inflate the value of the token through the use of their own funds and attract investors who in turn encourage other investors. This process can be completed within minutes or hours, and upon withdrawing the money, the same offender can then establish another token to target other unsuspecting investors.<sup>138</sup>

#### CASE STUDY: FRAUDULENT CRYPTOCURRENCY INVESTMENT



Members of an organized criminal group, most of whom were located in Belgium, were found to be engaged in an exit scam that the police believed had defrauded 223,000 individuals from 177 countries. The perpetrators operated from an otherwise legitimate social reward website and encouraged investment in a specific cryptocurrency. They employed a pyramid selling technique that rewarded members for recruiting new members to register. In this way, the fraudsters artificially inflated (or "pumped") the value of the investment. The organized criminal group either exited with a large amount of the funds before the bubble burst or used disinformation to inflate the value of the cryptocurrency before selling it to make a substantial capital gain. Members of the organized criminal group were found in possession of €1.1 million in cash and €1.5 million in cryptocurrencies.

Source: European Union Agency for Law Enforcement Cooperation (Europol), Cryptocurrencies: Tracing the Evolution of Criminal Finances, Europol Spotlight Report Series (Luxembourg, Publications Office of the European Union, 2021).

# Fraud by impersonation of a trusted individual or organization

Fraud by impersonation of a trusted individual or organization commonly involves the manipulation of communications to appear to be from a person or organization with whom victims have, or believe they have, an existing legitimate relationship. This includes public bodies such as the police or tax authority, service providers in the private sector and even friends or family members. A key distinguishing feature of many (but not all) types of fraud in this category is the use of persuasion techniques that appeal less to the wants and needs of victims (such as in consumer fraud) and instead evoke fear, dread, anxiety or worry. Inducing a heightened emotional state serves to impede decision-making and renders victims more susceptible to manipulation.

<sup>&</sup>lt;sup>137</sup> For example, see United States, Federal Bureau of Investigation, "Scammers target and exploit owners of cryptocurrencies in liquidity mining scam", 21 July 2022.

 $<sup>^{138}\,</sup>Pengcheng$  Xia and others, "Demystifying scam tokens on Uniswap decentralized exchange" (2021).

<sup>&</sup>lt;sup>139</sup> United States, Federal Trade Commission, Data and visualizations, Data spotlight, "Impersonation scams: not what they used to be", 1 April 2024.

<sup>&</sup>lt;sup>140</sup> DeLiema and Witt, Mixed Methods Analysis of Consumer Fraud Reports.

Fraud by impersonation involves a range of pretexts and scenarios, such as:

- Impersonating public officials. Perpetrators employ a range of techniques to masquerade as public officials representing agencies such as law enforcement entities, tax authorities or immigration, social security or health departments. This fraud commonly involves threats of legal repercussions or other forms of detriment should the victim not send a payment.<sup>141</sup>
- Impersonating legitimate services. Perpetrators employ a range of pretexts, ranging from debt collection and parcel deliveries to the provision of ICT support. They may even masquerade as bank officials seeking to prevent the loss of money to fraudsters. The fraudsters may purport to represent a service provider with whom the victim has an established relationship (e.g. a bank or courier service), or they may adopt an official-looking veneer to convince the victim that they are legitimate; for example, fraudsters who claim to represent a legal firm responsible for collecting a non-existent debt from the victim. 142 Other key examples include lottery and prize fraud, in which victims are told that they have won a lottery or other game and are persuaded to make a payment before being granted access to the funds. 143 Various reasons are given, including a purported processing, transfer or management fee or tax charges. However, once payment has been made, the victims do not receive the prize that was promised. Common techniques include the impersonation of a public authority, a known lottery or prize organization or an overseas lottery scheme. 144 In other examples, fraudsters claim to represent charities in mass-marketing campaigns to elicit donations from victims. 145 Persons in vulnerable contexts, including older persons and persons with disabilities, can be particularly at risk of these types of fraud due to their reliance on social services and higher levels of social isolation, as seen in the case study on consumer products and services and investment fraud in the previous chapter.
- Technical support fraud. This is highly prevalent in certain regions such as North America and Europe, with much of the offending emanating from India. 146 They commonly entail the fraudster impersonating a legitimate software company to convince victims that their machines are at risk and in need of technical support (e.g. a malware infection). The victims are then persuaded to provide remote access to their machine, before being asked for a fee to provide a fictitious service. 147 In some cases, additional charges are made on victims' accounts, malware is installed on their machines or their personal data may be stolen. Some fraudulent companies adopt methods that are similar to consumer fraud by mass-marketing technical support services through websites that mimic legitimate service providers.
- Impersonating a friend or family member. This typically involves messages that contrive a
  scenario in which the person is in some acute difficulty, such as being in hospital, having an
  accident or being arrested, and claims that it can be resolved if the victim sends a specified

<sup>&</sup>lt;sup>141</sup> One example involved a message sent by email and social media purporting to be from Europol telling victims that they had been seen accessing child sexual abuse material and needed to make a payment of between €3,000 and €7,000 to avoid prosecution (Europol, "Online fraud schemes: a web of deceit", Europol Spotlight Report Series (Luxembourg, Publications Office of the European Union, 2023), p. 11).

<sup>&</sup>lt;sup>142</sup> See, for example, United States, Federal Trade Commission, "Phantom debt collectors permanently banned from industry in FTC settlement", press release, 13 December 2021.

<sup>143</sup> Mortley, "A crime of opportunity".

<sup>144</sup> In one case, fraudulent communications were sent claiming to be from a company that had been appointed by the World Health Organization (WHO) to administer a lottery compensation scheme. The recipients were informed that they had been selected as beneficiaries or winners of a lottery compensation prize payment for losses and damages experienced during the COVID-19 pandemic (WHO, "Fraudulent 'COVID-19 Compensation Lottery Prize' scam, falsely alleges association with WHO and others", press release, 6 August 2021). See also United States, Federal Trade Commission, "Fake prize, sweepstakes, and lottery scams", May 2021.

<sup>&</sup>lt;sup>145</sup> For example, fraudulent schemes marketed using fraudulent web pages and emails, purporting to support Ukraine or Ukrainians affected by the armed conflict, in some cases spoofing humanitarian organizations' domains (see Europol, "Online fraud schemes").

<sup>&</sup>lt;sup>146</sup>Liu and others, "Understanding, measuring, and detecting". See also United States, Office of Public Affairs, "Dozens of individuals indicted in multimillion-dollar Indian call center scam targeting U.S. victims", press release, 27 October 2016.

<sup>&</sup>lt;sup>147</sup> Najmeh Miramirkhani, Oleksii Starov and Nick Nikiforakis, "Dial one for scam: a large-scale analysis of technical support scams", conference paper, Network and Distributed System Security Symposium held in San Diego, California, from 26 February to 1 March 2017.

amount of money. Often, the perpetrator pretends to be the victim's child or grandchild.<sup>148</sup> Some fraud schemes involve the use of personal details from social media posts of the friend or relative to make the communication more convincing, such as by knowing they are on holiday in a certain location. Emerging examples include offenders using generative artificial intelligence to clone a friend or relative's voice in a telephone call to the victim, creating an even more compelling or visceral response from the victim.<sup>149</sup>

The above-mentioned types of fraud commonly involve mass communication by means of spam email, social media, text messages or "robodialling", in which telephone calls are automated using a recorded message. These technologies facilitate near-simultaneous contact with thousands of victims at a time, giving them an immense reach. Some organized criminal groups operate from call centres, with call operators purporting to represent government bodies or known company brands. There is some evidence to suggest that older adults are targeted and particularly vulnerable to fraud such as government impersonation or technical support fraud. Support fraud.

## Identity fraud

Identity fraud involves the use of stolen or fake identity information to gain direct access to goods, services or monies from victims. Stolen information may be used to make purchases or access financial accounts. Identity fraud can be perpetrated without any direct communication with or action taken by the individual whose identity is being abused, because the deception is often directed at the provider of the goods, services or money (e.g. bank or commercial vendor). In this way the harm is spread across different actors, including the victim whose identity is abused, the financial service provider or other company from whom the monies are taken and, in some cases, the provider of the goods or services purchased using the stolen funds.

The manipulation and abuse of identity can serve a variety of different functions in the commission of organized crime other than to perpetrate fraud, not least to obstruct attempts to trace the criminality back to the perpetrators. <sup>152</sup> Similarly, it plays a key role in facilitating the deceptions employed in fraud types such as romance and consumer fraud. <sup>153</sup> The focus of the present section is the specific methodologies as part of which stolen or fake identity information is used 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. The victim in many of these cases is the business that is tricked into supplying finance, goods or services to the fraudster.

Importantly, the perpetration of identity fraud is not contingent on the involvement of organized criminal groups. For example, the impersonation of a cardholder requires little more than a snatched bag and a local shop to make a quick purchase. However, the capacity to perpetrate identity fraud at scale and achieve high profits is greatly augmented by the skills and resources available to organized

<sup>&</sup>lt;sup>148</sup> United States, Federal Bureau of Investigation, "The grandparent scam: don't let it happen to you", 2 April 2012.

<sup>&</sup>lt;sup>149</sup> Alvaro Puig, "Scammers use AI to enhance their family emergency schemes", Federal Trade Commission, 20 March 2023.

<sup>&</sup>lt;sup>150</sup>A common example consists of the use of fraudulent messages that claim to be from the social security administration. In 2020, such a scheme targeted nearly half of all adults in the United States over a three-month period (DeLiema and Witt, *Mixed Methods Analysis of Consumer Fraud Reports*, p. 2).

<sup>&</sup>lt;sup>151</sup>Liu and others, "Understanding, measuring, and detecting"; Lei Yu and others, "Vulnerability of older adults to government impersonation scams", *JAMA Network Open*, vol. 6, No. 9 (September 2023); and DeLiema and Langton, "Older victims of mass marketing scams".

<sup>152</sup> Baechler, "Document fraud".

<sup>&</sup>lt;sup>153</sup> See, for example, Cassandra Cross and Rebecca Layt, "I suspect that the pictures are stolen': romance fraud, identity crime, and responding to suspicions of inauthentic identities", *Social Science Computer Review*, vol. 40, No. 4 (August 2022).

criminal groups. This threat is rendered particularly acute by the proliferation of available targets within growing digital economies.

There are different forms of identity information that can be acquired, and each can be exploited in different ways: personal information that makes up digital identities across different online environments such as names or dates of birth; financial account data such as credit card numbers; online account information such as usernames and passwords; and biometric data such as a digital fingerprint stolen from an electronic device. 154

Stolen data can be used to purchase goods and services, submit applications for loans and other finance or access and transfer money from victims' accounts. The resources and techniques that can be employed by fraudsters to gain access to personal information include the following:

- System intrusion. Some fraudsters are active in the acquisition of personal information by means of illicit hacking techniques, the deployment of malware, or phishing (see the section on identity theft below for more detail).
- Online criminal markets. There is a vibrant underground economy involved in the buying and selling of personal data that 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.
- Social engineering. This is often achieved by an advertisement or other unsolicited communication by email or other online means, text message or an unsolicited telephone 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 provide offenders with direct access to online accounts (see case study below).

A range of techniques are employed to perpetrate identity fraud. The key methods are account takeover, card-not-present and application fraud.

### Account takeover fraud

In account takeover fraud, the criminals acquire legitimate credentials to access user accounts. These can include bank accounts but also other types of financial account (e.g. virtual currency providers), retail sites or any providers of goods and services. The use of the victims' stolen account credentials means that the offender's transactions or other activities become difficult to distinguish from those of the real account holder. The account can be leveraged for several purposes, including a direct transfer of funds to accounts controlled by the offenders and use of the account to fraudulently purchase goods or services. In some instances, the acquisition of information to access a victim's account is the first in a sequence of steps required to access the monies, good or services, including subsequent forms of system intrusion. Those steps include adaptations to overcome two-factor authentication intended to prevent illegitimate access to accounts. This has prompted offenders to deploy additional techniques and technologies, including:

SIM-swapping, which involves tricking a telecommunications provider into porting a victim's
telephone number to a SIM card in the possession of the offender. This provides the means
for offenders to bypass the two-factor authentication protections of financial service providers
to gain direct access to an account. One group in Spain was able to make fraudulent transfers

<sup>&</sup>lt;sup>154</sup> Europol, "Online fraud schemes"; and Bert-Jaap Koops, Katja de Vries and Mireille Hildebrandt, eds., D7.14b: Idem-Identity and Ipse-Identity in Profiling Practices, Future of Identity in the Information Society Report, No. 507512 (2009).

<sup>155</sup> Yip, Shadbolt and Webber, "Why forums?".

to the value of  $\in 3$  million by deploying a banking trojan or other malware to gain access to victims' online banking credentials, applying to telecommunications providers for a duplicate of the victims' SIM cards to intercept the authentication codes sent by the bank and then transferring funds to money mules' accounts.<sup>156</sup>

Targeting alternative payment methods, such as the "tokenized" credit cards used for mobile
payment services and in digital wallets, whereby offenders are able to intercept the one-time
passwords sent by banking institutions to authorize a transfer of funds and thereby make
purchases or obtain money.<sup>157</sup>

It is common for funds to be taken from accounts using digital transfers to accounts controlled by offenders. However, organized criminal groups can also gain possession of physical identifiers such as bank cards or fake identification to physically attend the bank and withdraw money.<sup>158</sup>

## CASE STUDY: BANKING FRAUD



In the Kingdom of the Netherlands, a group targeted two banks with a view to gaining access to customer bank accounts. The group was made up of eight core members and other, peripheral individuals who facilitated the fraud. A phishing email was sent asking customers to provide information or click a link that sent them to a website controlled by the offenders that spoofed the bank's official website. In this way, they acquired customers' details for accessing their online bank accounts. A few days later, the offenders made a telephone call to victims and told them that new security measure had been implemented at the bank and requested that they provide the one-time transaction code to ensure that their account was secure. Once the code was provided, the offender made a series of bank transfers from the customers' accounts. The money was transferred to the accounts of money mules so as to break the financial trail, and the money was then swiftly withdrawn.

Source: Eric Rutger Leukfeldt, "Cybercrime and social ties: phishing in Amsterdam", Trends in Organized Crime, vol. 17, No. 4 (December 2014).

## Card-not-present fraud

Card-not-present transactions are unauthorized purchases made remotely from a vendor, either online or over the telephone. The acquisition of a victim's financial credentials is sufficient to deceive both the financial service provider and the commercial vendor, with no need for a direct interaction with the victim or to gain access to the physical payment card. There is a booming underground economy in which cybercriminals with the abilities to acquire this information in bulk (e.g. by means of a data breach) can sell it to would-be fraudsters for a profit. To illustrate, a website investigated by the police was found to contain 150,000 stolen credit card numbers from 1,300 banks, mostly obtained by means of system intrusion; the sale of these data to fraudsters had resulted in \$20 million being lost from accounts held in the United States.<sup>159</sup> A number of key steps are typically required by identity

<sup>156</sup> Europol, Internet Organised Crime Threat Assessment 2020 (Luxembourg, Publications Office of the European Union, 2020), p. 44.

<sup>&</sup>lt;sup>157</sup> Europol, "Online fraud schemes", p. 15.

<sup>&</sup>lt;sup>158</sup> See, for example, UK Finance, "Organised crime group sentenced following over £1 million conspiracy to defraud", press release, 6 November 2023.

<sup>&</sup>lt;sup>159</sup> United States of America v. Burkov, available from the SHERLOC knowledge management portal.

fraudsters to exploit a victim's financial credentials, some of which may involve other co-offenders, including those online or living in the same locality. Key stages include:

- Acquiring knowledge and resources from other members of online groups.
- Acquiring financial credentials from online groups.
- Disguising orders to avoid triggering fraud-detection algorithms on a commercial site. This may entail placing multiple smaller orders to blend in with legitimate orders.
- Receiving the orders at an address that cannot be traced to the fraudsters it may be an
  unoccupied property or the address of a "mule". Alternatively, an insider within the delivery
  company may be used to intercept the item.
- Reselling the items as an individual seller or selling them in bulk by impersonating a legitimate merchant in mainstream online marketplaces.<sup>160</sup>

### CASE STUDY: CARD-NOT-PRESENT FRAUD



A network of offenders used stolen credit card data to make fraudulent purchases on commercial websites. They acquired these data in two ways: (a) sourcing and purchasing them from online carding forums; and (b) stealing the information from a former employer. The offenders were also found in possession of automatic teller machine (ATM) skimmers<sup>a</sup> that could be used to collect more card details. A key preparatory step was to hack into customer accounts on commercial websites and amend their contact information, meaning that cardholders would not be notified of the purchases made by the offenders. Products were purchased and delivered to parcel collection points and collected using fake identity cards or "mules" enlisted to collect the packages. The police identified approximately 2,000 orders placed on shopping websites, with an estimated value of up to €60,000. The goods were then resold on commercial websites.

Source: Paris Tribunal de grande instance, Judgment, 20 November 2018 (TGI Paris, 13e ch. corr., jugement du 20 novembre 2018), available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

# Application fraud

In a similar vein to card-not-present fraud, application fraud exploits the widespread availability of personal information, but with the aim of applying 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 need to access a composite of personal information (e.g. name, address and date of birth) to be able to credibly impersonate another 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 to become more creditworthy before being used to submit applications for high-value financial products. The association between organized crime and mortgage fraud has long been recognized and is commonly facilitated by professionals such as mortgage brokers, real estate appraisers, accountants, solicitors and escrow agents. Mortgage fraud provides a means of laundering the proceeds from another crime (e.g. drug supply) but can also be used to generate a criminal profit. Common methods include taking out

 $<sup>^{\</sup>it a}$  A piece of hardware that is attached to an ATM to steal card information.

<sup>&</sup>lt;sup>160</sup> Bodker and others, "Card-not-present fraud".

<sup>&</sup>lt;sup>161</sup> May and Bhardwa, Organised Crime Groups Involved in Fraud; and Reurink, Financial Fraud.

mortgages using another person's details or the details of a deceased person, or taking out multiple mortgages on a single address. 162

# Relationship and trust fraud

The processes for establishing trust play a critical role in any type of fraud. However, in the case of relationship and trust fraud, the fraudsters use specific techniques to foster and exploit the power of a personal relationship to develop the trust needed to manipulate and deceive victims. <sup>163</sup> In this type of fraud, the victim does not expect to receive a product or service but instead has the expectation of forming a genuine relationship with the offender. <sup>164</sup> The complexity of the fraud lies less in the exploitation of technical or technological systems and more in the dynamics of the relationship between the victim and the perpetrator.

Many fraudsters establish relationships online and use a variety of social engineering techniques over a period of months or even years to gain a victim's trust. The victims commonly expect a romantic relationship, but the relationship can also 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. Further intersectional characteristics such as citizenship status or disability status can lead to increased vulnerability to such crimes. Criminals target and exploit this vulnerability through a process of befriending or romantic engagement by visiting the victim in person (e.g. by posing as tradespersons), speaking over the phone or communicating online. 165

Irrespective of the victims' characteristics, the impact of relationship and trust fraud can be considerable. Although victims experience financial losses, they also suffer as a result of broken trust and the loss of a significant personal relationship. <sup>166</sup> In addition, they may experience significant psychological and emotional harm. Some may even refuse to accept that they are or have been a victim of fraud.

## Romance fraud

A common form of relationship and trust fraud is romance fraud, whereby offenders construct relationships online to facilitate deception with the intention of tricking victims into sending them money. <sup>167</sup> The financial losses to individuals can be significant (see the case study below). It affects 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 is commonly on social media or dating websites or applications by an offender using a false identity, along with a corresponding profile narrative. <sup>168</sup> A single offender may switch between identities to target and entice prospective victims; for example, a seductive female profile image to attract heterosexual men

<sup>&</sup>lt;sup>162</sup> May and Bhardwa, Organised Crime Groups Involved in Fraud.

<sup>&</sup>lt;sup>163</sup> Cassandra Cross, "Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud", Current Issues in Criminal Justice, vol. 36, No. 3 (2024).

<sup>&</sup>lt;sup>164</sup> Beals, DeLiema and Deevy, "Framework for a taxonomy of fraud".

<sup>&</sup>lt;sup>165</sup> Cassandra Cross, "They're very lonely': understanding the fraud victimisation of seniors", *International Journal for Crime, Justice and Social Democracy*, vol. 5, No. 4 (2016); and Phillips, "From 'rogue traders' to organized crime groups".

<sup>&</sup>lt;sup>166</sup> Monica T. Whitty and Tom Buchanan, "The online romance scam: a serious cybercrime", *Cyberpsychology, Behavior and Social Networking*, vol. 15, No. 3 (March 2012).

 $<sup>^{\</sup>rm 167}$  Coluccia and others, "Online romance scams".

<sup>&</sup>lt;sup>168</sup> Cross and Layt, "'I suspect that the pictures are stolen".

or a male profile that presents the individual as elite, glamorous and trustworthy (such as a member of the military). <sup>169</sup> The following seven key stages are commonly seen in romance fraud:

- The victim's desire to find a partner
- The presentation of an ideal profile to the victim
- The grooming process
- The sting
- The continuation of the scam
- Sexual abuse
- Retargeting<sup>170</sup>

Once the relationship is established, the offender may initially ask for a small sum of money, before asking for larger amounts, often citing a crisis scenario that serves to apply pressure and urgency to the victim (e.g. a health emergency or urgent travel requirement).<sup>171</sup> If sexual images were exchanged, money may also be extorted from the victim. The victims are commonly asked to transfer money to third countries or by using a gift card or prepaid card and may subsequently be targeted with other types of fraud or even enlisted to help defraud other victims (e.g. used as a money mule).<sup>172</sup>

# Crypto-confidence investment fraud

A more recent type of fraud has seen romance fraud converge with cryptocurrency investment fraud. Crypto-confidence investment schemes (or, as many in the media have named them, "pig-butchering" fraud)<sup>173</sup> involve an offender fostering a personal relationship with a victim online. Instead of fabricating a crisis scenario, the offenders establish an intimate relationship with the victim and then exploit the trust gained to lure the victims into a fraudulent investment scheme. The offenders may develop a fraudulent website or application that can be accessed by the victim, and even provide "customer service" for investors. 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 that they are victims of fraud, and introduces further difficulties for criminal investigators to trace the funds back to offenders. The integration of the deception has a number of consequences of 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 that they are victims of fraud, and introduces further difficulties for criminal investigators to trace the funds back to offenders.

Much of the research into romance fraud has been focused on the victims and their experiences, not on the offenders, who are less visible. Many are transnational crimes, and they are often (but not always) perpetrated by organized criminal groups. The case study on romance fraud below provides an example where an organized criminal group targeted a victim across international borders over an extended period of time.

 $<sup>^{169}</sup>$  Suleman Lazarus and others, "What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021)", Journal of Economic Criminology, vol. 2 (2023).

<sup>&</sup>lt;sup>170</sup> Monica T. Whitty, "The scammer's persuasive techniques model: development of a stage model to explain the online dating romance scam", *The British Journal of Criminology*, vol. 53, No. 4 (July 2013).

<sup>&</sup>lt;sup>171</sup> Cassandra Cross and Thomas J. Holt, "The use of military profiles in romance fraud schemes", Victims and Offenders, vol. 16, No. 3 (2021).

<sup>&</sup>lt;sup>172</sup> Europol, "Online fraud schemes".

<sup>&</sup>lt;sup>173</sup> The use of this phrase is not recommended owing to the negative connotations for the victims.

<sup>1&</sup>lt;sup>74</sup> 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).

<sup>&</sup>lt;sup>175</sup> Cross, "Romance baiting, cryptorom and 'pig butchering'".

<sup>&</sup>lt;sup>176</sup>Lazarus and others, "What do we know about online romance fraud studies?".

### CASE STUDY: ROMANCE FRAUD



Three perpetrators targeted a female living in Australia over a period of three years. Initial contact was made on a matchmaking website before maintaining contact by email and over the telephone. The offenders adopted the identity of a German citizen living in Australia but working from Ghana. To elicit funds from the victim, they presented multiple scenarios over time, ranging from a need for assistance to clear imported goods at a port to experiencing health problems. At various stages, the initial offender introduced the victim to other offenders, claiming that they were his business associates; she communicated with each of them and was asked to provide financial assistance to remedy an urgent situation. The victim was motivated to assist the initial offender, with whom she believed she was in a relationship, in returning to Australia. In total, the victim was defrauded of nearly 450,000 Australian dollars.

Source: Republic v. Mohammed Libabatu, Charles Mensah and Nurudeen Alhassan, available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

# Fraud against businesses or organizations

Fraud against businesses or organizations typically involves the abuse of internal systems or a commercial relationship to defraud the victim. The fraud can be perpetrated by someone internal or external to the organization, such as personnel, clients or suppliers, insiders in collusion with external perpetrators, or external criminals who exploit the business's or organization's services or systems. This type of fraud may be perpetrated from within otherwise legitimate enterprises, actors or products, rather than being schemes that are designed from the outset to perpetrate fraud.

Fraud perpetrated by internal personnel typically involves the abuse of internal systems or a commercial relationship to defraud an employer, business partner or other stakeholder. This type of fraud includes major corporate fraud, which is commonly perpetrated by personnel in management positions who deceive investors or other key stakeholders. Financial statement fraud encapsulates a variety of methods for misrepresenting the true nature or financial health of a company, fund or investment product in order to mislead and distort the perceptions of others, such as investors, regulators and other market actors, about its financial health and future prospects. Similar types of accounting fraud may also cover up the misappropriation, misapplication or embezzlement of funds. Such fraud may be perpetrated in response to pressures to meet performance expectations and may be carried out by corporate executives, financial traders or hedge fund managers reporting on financial performance.

The criminal motivation for this type of fraud can stem from a variety of circumstances, some of which arise from the conditions in the company or sector. Examples include company directors responding to financial difficulty or a workplace culture that fosters a permissive attitude to fraud or that imposes high expectations and pressure to achieve financial results. In many instances of fraud against businesses or organizations, delineating fraudulent and legitimate (although ethically dubious) practices can be a challenge.

Fraud against businesses or organizations is often aimed at defrauding a particular business or organization but can in some cases have a more far-reaching impact on the sector, including on consumers

 $<sup>^{\</sup>rm 177}$  Duffield and Grabosky, The Psychology of Fraud.

<sup>&</sup>lt;sup>178</sup> Paolo Campana, "When rationality fails: making sense of the 'slippery slope' to corporate fraud", *Theoretical Criminology*, vol. 20, No. 3 (August 2016). See also United States, Department of Justice, Criminal Division, "Securities and commodities fraud", 11 August 2023.

<sup>179</sup> Reurink, Financial Fraud.

in the market. It is not uncommon for this type of fraud to occur over prolonged periods of time, and it can lead to substantial financial losses for businesses and organizations. However, the low sentences handed to white-collar fraudsters and the greater capacity among fraudsters in legitimate and trusted positions to perpetrate serious fraud without recourse to co-offenders may limit the role of organized criminal groups in certain contexts. <sup>180</sup>

Fraud involving external actors who exploit trading or other commercial relationships with the victim business or organization includes:

- Long- or short-firm fraud, which can be perpetrated by existing trading companies or companies that are 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. This is done knowing that they either cannot pay or have no intention of making payment. Some fraudsters abuse the trust systems that facilitate international trade. Letters of credit are commonly used to make payment in international trade, whereby a bank acts as guarantor for the buyer in a transaction. Fraudulent buyers set up their own fake banking institutions to act as their guarantors to defraud sellers. The goods are shipped by the sellers, who then receive no payment.
- Procurement or supplier fraud, which encompasses a variety of methods to secure business contracts or payment for goods and services. This can involve suppliers submitting false statements<sup>183</sup> or, in some cases, the corruption of staff members who expect payment for providing the contracts and funds, and thereby acquire the goods and services by means of deception. In one example, a construction company in the Kingdom of the Netherlands entered into a real estate contract with a pension fund but, over a 10-year period, the contract managers inflated the contracts by millions of euros.<sup>184</sup>

## CASE STUDY: FINANCIAL STATEMENT FRAUD



Perpetrators from multiple banks in Germany, France and the United Kingdom of Great Britain and Northern Ireland had sought to manipulate the Euro Interbank Offered Rate (Euribor). These published rates are the estimates that are provided by the banks on the cost of borrowing from other banks on the interbank market on a specific day. The rates are then used as a benchmark for their loan operations and influence the interest rates for the loans, mortgages and savings accounts provided to customers. The convicted offenders submitted false interest rate estimates with the intention of moving the benchmark in the direction that would benefit their employer or themselves the most. The criminal proceeds were considerable, with one co-offender personally earning £57.8 million from the manipulation of the rates. Moreover, their actions served to undermine the integrity of the financial system.

Sources: United Kingdom, Serious Fraud Office, "Senior bankers sentenced to 9 years for rigging EURIBOR rate", 1 April 2019; and Ruben Herrera and others, "The manipulation of Euribor: an analysis with machine learning classification techniques", Technological Forecasting and Social Change, vol. 176, art. No. 121466 (March 2022).

<sup>&</sup>lt;sup>180</sup> Levi, "Organized fraud and organizing frauds"; and Levi, "Hitting the suite spot".

<sup>&</sup>lt;sup>181</sup> Michael Levi, "The craft of the long-firm fraudster: criminal skills and commercial responses", in *Crime at Work: Increasing the Risk for Offenders*, vol. 2, Martin Gill, ed. (London, Palgrave Macmillan, 1998).

<sup>182</sup> Reurink, *Financial Fraud* 

<sup>&</sup>lt;sup>183</sup> For example, a group of four fraudsters systematically defrauded an e-commerce platform by manipulating the vendor system to induce the corporation into paying for goods it had not ordered (United States Attorney's Office, Southern District of New York, "Four individuals charged with \$19 million fraudulent invoicing scheme targeting Amazon's vendor system", press release, 19 August 2020).

<sup>&</sup>lt;sup>184</sup> Philip Gounev, Tihomir Bezlov and European Commission, Directorate-General for Migration and Home Affairs, *Examining the Links between Organized Crime and Corruption* (Brussels, Publications Office, 2010), p. 121.

### CASE STUDY: LONG-FIRM FRAUD



The chief executive officer and two senior executives at a steel trading company in the United Kingdom of Great Britain and Northern Ireland defrauded 20 trade finance banks from multiple countries of \$500 million. Over a period of two years, they secured short-term loans by providing misleading information and false contracts for non-existent steel shipment orders. They used an in-house shipping company that was registered overseas to certify the false shipping documents. The loans bolstered the company's finances, which allowed them to continue trading. The company avoided making repayments on the loans until it eventually collapsed, leaving large amounts of unpaid debt with the banks. The co-offenders were convicted and the chief executive officer was given a six-and-a-half-year prison sentence.

Source: United Kingdom, Serious Fraud Office, "Serious Fraud Office secures three convictions in \$500 million trade finance fraud", 2 February 2023.

Organized criminal groups can also defraud businesses without occupying a legitimate or ostensibly legitimate position in business. Instead, these types of fraud are perpetrated either by means of system intrusion by cybercriminals or by abusing the services that the victim organization provides to customers.

# Business email compromise fraud

Business email compromise fraud targets corporations, small businesses and organizations from a range of sectors. It is one of the most prevalent forms of organized fraud globally. The fraudsters employ various social engineering techniques to persuade personnel to make unauthorized transfers of funds to accounts controlled by the offenders. The first step is to infiltrate the communication systems of an organization to help persuade the recipients that the emails sent are legitimate: key methods include hacking the email accounts of staff members, sending phishing emails to elicit the account details of staff members and exploiting communications providers to impersonate domain names that are familiar to the target organization. Various narratives are adopted by offenders, including 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 and impersonating a lawyer requesting a wire transfer to address a sensitive matter. Communication can occur over a period of time and the offenders may invest time in understanding the organization and its systems in order to defraud it on multiple occasions (see case studies below).

### Crash-for-cash fraud

Crash-for-cash fraud involves criminal groups that systematically defraud vehicle insurance companies. R range of methods are used, including submitting false reports of accidents in order to claim insurance money and, in more serious cases, causing car accidents involving innocent members of the public to claim against their insurance. Reports of the public to claim against their insurance.

<sup>&</sup>lt;sup>185</sup> INTERPOL, "INTERPOL global financial fraud assessment".

<sup>&</sup>lt;sup>186</sup> Norah S. 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", in 2020 Anti-Phishing Working Group (APWG) Symposium on Electronic Crime Research (eCrime) (Boston, United States, 2020).

<sup>&</sup>lt;sup>187</sup> Alessandro E. Agazzi, "Business email compromise (BEC) and cyberpsychology" (2020).

<sup>&</sup>lt;sup>188</sup> Mark Button and others, "Just about everybody doing the business? Explaining 'cash-for-crash' insurance fraud in the United Kingdom", *The Australian and New Zealand Journal of Criminology*, vol. 50, No. 2 (June 2017).

<sup>&</sup>lt;sup>189</sup> Mark Button and Graham Brooks, "From 'shallow' to 'deep' policing: 'crash-for-cash' insurance fraud investigation in England and Wales and the need for greater regulation", *Policing and Society*, vol. 26, No. 2 (2016).

### CASE STUDY: BUSINESS EMAIL COMPROMISE



A business email compromise fraud targeting a business in the United States of America resulted in the loss by the business of \$1 million. The fraudsters were a group of three co-offenders, two of whom were located in Nigeria. The offenders impersonated another United States-based business with which the victim had an existing business relationship. They sent an initial email requesting payment for services that the business had provided, and a second email requesting that the money be sent to an alternative bank account, purportedly for tax reasons. The bank account was owned by an individual located in another country. The profits were believed to have been shared among the three co-offenders.

Source: Nigerian Financial Intelligence Unit, "Nigeria releases money-laundering typologies through fraud report", 12 August 2023.

## CASE STUDY: BUSINESS EMAIL COMPROMISE



The offenders sent a phishing email to the chief financial officer of a company that appeared to provide a link to the company's ICT service login page. Having clicked on the link, the victim was taken to a web page that resembled the legitimate page. The financial officer entered his login credentials, which were then captured by the offenders and used to access his email account. They were able to then impersonate the victim and send emails to other members of the financial team, requesting a number of wire transfers to accounts in their control. Furthermore, they observed and learned about the policies and practices in the company and were able to imitate an email and invoice that would typically be received from a legitimate vendor. The fake invoices were paid to accounts controlled by the offenders. The company suffered financial losses of approximately \$11 million.

Source: United States of America v. Okeke, available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

Fraud is highly diverse, encompassing a daunting range of methods and techniques for employing deception to make a criminal gain. Furthermore, the methods employed by fraudsters continuously evolve to exploit criminal opportunities that emerge from advancements in communications, commerce, finance and technology. Corralling the diverse methods into a single framework for understanding the problem is a considerable challenge, but essential to the development of comprehensive and cohesive public policies for tackling organized fraud. This typology provides an important step in developing a framework for conceptualizing this multifaceted crime.



# CHAPTER III

# Organized fraud offenders

Criminals involved in organized fraud vary in both their characteristics and the pathways they take into offending. This variety is rooted in the wide-ranging methods (and requisite capabilities) that are used to perpetrate fraud, the range of different settings in which fraud can emerge, including the different social, economic and political environments in different global regions, and the variety of roles and motivations of individual fraudsters. It is important to understand who perpetrates organized fraud and the pathways that are taken into this type of offending so as to target interventions that are effective in deterring and diverting individuals from these crimes.

Fraud offenders are a hidden and hard-to-reach population, and research on them is still developing. The present section contains a compilation of evidence to discuss, first, the significance of co-offending, second, the characteristics of organized fraud offenders, and third, the motivations for perpetrating these crimes.

# Role and significance of co-offending

Pathways into organized crime are in part determined by the criminal opportunities that emerge out of everyday and proximate activities, environments and trusted relationships (e.g. social and professional networks). <sup>190</sup> The capacity to meet and forge trusted relationships with like-minded persons can increase the scope for offending in ways that might otherwise be out of reach. <sup>191</sup> This includes co-offenders who have resources or capabilities that are more limited in availability (e.g. professional enablers or cybercriminals with technical expertise) <sup>192</sup> and others with more generalized capabilities (e.g. call centre operators or money mules). Identifying the resources and capabilities required to perpetrate different types of fraud can help identify groups that are vulnerable to being drawn into organized crime: examples include the potential for legal professionals to be corrupted and for students to be recruited as money mules. <sup>193</sup>

<sup>&</sup>lt;sup>190</sup> Edward R. Kleemans and Henk G. van de Bunt, "Organised crime, occupations and opportunity", *Global Crime*, vol. 9, No. 3 (2008); Edward R. Kleemans and Henk G. van de Bunt, "The social embeddedness of organized crime", *Transnational Organized Crime*, vol. 5, No. 1 (1999); and Markus Felson, *The Ecosystem for Organized Crime*, European Institute for Crime Prevention and Control, affiliated with the United Nations, Paper, No. 26 (Helsinki, 2006).

<sup>&</sup>lt;sup>191</sup> Edward R. Kleemans and Christianne J. de Poot, "Criminal careers in organized crime and social opportunity structure", *European Journal of Criminology*, vol. 5, No. 1 (January 2008).

<sup>&</sup>lt;sup>192</sup> Jason R.C. Nurse and Maria Bada, "The group element of cybercrime: types, dynamics, and criminal operations", in *The Oxford Handbook of Cyberpsychology*, Alison Attrill-Smith and others, eds. (Oxford, Oxford University Press, 2019).

<sup>&</sup>lt;sup>193</sup> Australian Transaction Reports and Analysis Centre, "Combating the exploitation of international students as money mules: financial crime guide" (2024); and May and Bhardwa, *Organised Crime Groups Involved in Fraud.* 

The locations in which prospective co-offenders can meet are significant, because without such points of convergence, co-offenders are less likely to meet and organized crime is less likely to occur. The availability and accessibility of these points of convergence is significant in determining who becomes involved in organized crime and how it takes shape. <sup>194</sup> Particularly salient in the context of cyberfraud is the growth in online communications on both the open and dark web, which provide spaces for offenders to converge, communicate and trade with other criminals (see case study below). The online criminal markets and forums that provide a place for criminals (including fraudsters) to exchange resources and knowledge are a key example of this. <sup>195</sup> From these settings, the crime-as-a-service model has emerged, an underground economy in which cybercriminal entrepreneurs can profit from supplying technical tools, resources and services to fraudsters (and other offenders). <sup>196</sup> Key products and services that are available to purchase or hire include stolen personal data, phishing and spamming services, money-laundering services (including money mules), account hacking and the supply of botnets. <sup>197</sup>

Technology has created new opportunities for would-be fraudsters to form organized criminal groups from a global pool of prospective co-offenders. Furthermore, it provides a gateway to co-offending and organized crime that is accessible to would-be fraudsters. The anonymity of online spaces mitigates the risks involved in cooperating with unknown actors, and new members can quickly establish themselves and build status in these online communities. Alliances may be ephemeral, existing solely to facilitate the completion of a specific task, or these new technologies may foster longer-lasting collaboration.

Relationships formed offline remain a key characteristic of organized criminal groups that engage in cyberfraud and often represent the more stable and durable elements of a group.<sup>200</sup> This includes organized criminal groups that expand their criminal repertoire to include fraud, or associates who come together for the purpose of perpetrating fraud. These groups can become hybridized by integrating into the online underground economy to access criminal resources and co-offenders.<sup>201</sup> Organized fraud entails complex methods of offending, commonly involving an extended sequence of actions and events that are often separated from one another in time and space,<sup>202</sup> which can in turn attenuate the relationships between the different offenders positioned along that sequence.<sup>203</sup> The result is that tasks are distributed across a multitude of loosely connected criminal actors, which increases their capacity to specialize and garner expertise. Furthermore, a more even distribution of tasks and roles across members of an organized criminal group serves to spread culpability and the risk of detection by law enforcement entities.

<sup>&</sup>lt;sup>194</sup> Felson, *The Ecosystem for Organized Crime*; and Kleemans and de Poot, "Criminal careers in organized crime".

<sup>&</sup>lt;sup>195</sup> Soudijn and Zegers, "Cybercrime and virtual offender convergence settings"; and Yip, Webber and Shadbolt, "Trust among cybercriminals?".

<sup>&</sup>lt;sup>196</sup> INTERPOL, "INTERPOL global financial fraud assessment", p. 11.

<sup>&</sup>lt;sup>197</sup> Akyazi, van Eeten and Gañán, "Measuring cybercrime as a service (CaaS)"; An and Kim, "A data analytics approach"; Jirovsky and others, "Cybercrime and organized crime"; and INTERPOL, "INTERPOL global financial fraud assessment" p. 11.

<sup>&</sup>lt;sup>198</sup> Soudijn and Zegers, "Cybercrime and virtual offender convergence settings".

<sup>&</sup>lt;sup>199</sup> Odinot and others, Organised Cybercrime in the Netherlands; and Yip, Shadbolt and Webber, "Why forums?".

<sup>&</sup>lt;sup>200</sup> Leukfeldt, Lavorgna and Kleemans, "Organised cybercrime or cybercrime that is organised?"; Lusthaus and others, "Cybercriminal networks in the United Kingdom and beyond"; and Odinot and others, *Organised Cybercrime in the Netherlands*.

<sup>&</sup>lt;sup>201</sup> Roderic Broadhurst and others, "Crime in cyberspace: offenders and the role of organized criminal groups", Working Paper (Canberra, Australian National University Cybercrime Observatory, 2013); and Choo, "Organized crime groups in cyberspace".

<sup>&</sup>lt;sup>202</sup> Klaus von Lampe, "Situational prevention of 'organised crime': preventing phantom conceptions with phantom means?", in *Cross-border Crime Inroads on Integrity in Europe*, Petrus C. van Duyne and others, eds. (Nijmegen, Kingdom of the Netherlands, Wolf Legal Publishers, 2010).

<sup>&</sup>lt;sup>203</sup> For example, identity fraud requires the theft of personal data, the establishment of an online forum on which to sell the information, the acquisition of the data by fraudsters, the selection and purchase of products and services from a platform, the enlisting of mules to receive the stolen items and the reselling of the items for financial gain (Bodker and others, "Card-not-present fraud").

### CASE STUDY: CRIMINAL MARKETPLACE



Genesis Market provided an online meeting point for criminals to trade in digital identities. The marketplace offered for sale bots that had infected the devices of victims by means of either malware or an account takeover attack. The price of each bot would vary depending on the amount and quality of the data collected (account details for accessing online bank accounts were the most highly valued). Criminals who purchased the bots were provided with the data and with software called "browser fingerprints", which enabled them to mimic the behaviour of the victims when accessing the account and bypass the anti-fraud security measures on the platform. Criminals from all over the world accessed the marketplace, and it was estimated that 80 million credentials stolen from 2 million people had been hosted on the site.

Source: European Union Agency for Law Enforcement Cooperation (Europol), "Takedown of notorious hacker marketplace selling your identity to criminals", 5 April 2023.

## CASE STUDY: CRIME AS A SERVICE



A criminal website supplied the iSpoof software, which enabled criminals to make telephone calls that appeared to come from trusted entities such as banks, retail companies and government institutions. This allowed criminals to more credibly impersonate legitimate organizations when contacting victims, thereby facilitating the deception. The website was marketed to criminals through the encrypted messaging application Telegram and at one time had up to 59,000 users across the world who paid a monthly fee to access its services. There were multiple administrators, but one individual based in the United Kingdom of Great Britain and Northern Ireland had played a leading role in creating the software and administrating the website. Over a period of 16 months, the website earned over €3.7 million, and a large proportion of those gains went to the lead administrator.

Sources: European Union Agency for Law Enforcement Cooperation (Europol), "Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests", 24 November 2022; and "Fraudster jailed for running multimillion-pound website iSpoof", The Guardian, 19 May 2023.

# Characteristics of organized fraud offenders

There is no typical fraudster. As criminal opportunities expand, particularly in the context of cyberfraud, the pathways and profiles across the globe continue to diversify. The various methods for perpetrating fraud emerge from within different social, commercial, financial and technological settings, each calling for particular resources or capabilities, which means that the pathways and characteristics of fraudsters can also vary within the multitude of settings.

Historically, most fraud has been committed from within white-collar settings. In this context, the perpetrators are typically otherwise law-abiding individuals who choose to exploit opportunities that arise from within a legitimate working environment – for example, embezzlement, bankruptcy or tax fraud.<sup>204</sup> In the context of organized crime, white-collar fraud offenders normally have little prior

<sup>&</sup>lt;sup>204</sup> Victor R. van der Geest, David Weisburd and Arjan A.J. Blokland, "Developmental trajectories of offenders convicted of fraud: a follow-up to age 50 in a Dutch conviction cohort", *European Journal of Criminology*, vol. 14, No. 5 (September 2017). It should be noted that tax fraud is not within the scope of the present issue paper.

contact with criminal justice systems before their conviction for organized fraud, and tend to be older than other persons involved in organized crime.<sup>205</sup> This is likely because the opportunities to perpetrate white-collar fraud are more restricted to individuals within established legitimate occupations who are able to cross the thin margins that separate licit and illicit practices.<sup>206</sup> White-collar fraudsters continue to represent a significant element of the organized fraud problem (see the section on fraud against businesses or organizations in chapter II above); however, the evidence suggests a much greater diversity in pathways taken into organized fraud, and in the characteristics of the perpetrators. It is also important to recognize the involvement of both men and women in organized fraud. Due to prevailing stereotypes related to organized crime, women are seen predominantly as victims and rarely as perpetrators. However, research has indicated that the reality is more complex and that men and women can be both perpetrators and victims of organized fraud.<sup>207</sup>

Conceptualizations of white-collar crimes have become less rooted in certain categories of offender (e.g. those from the upper classes) and instead focused on certain types of offence that involve the violation of trust.<sup>208</sup> There are many types of organized fraud in which a business is established (or comes to be used) for the sole purpose of perpetrating fraud. A business provides a legitimate front to facilitate the deception of victims and the authorities; prominent examples include call centres (or "boiler rooms") for engaging with the public, and commercial businesses that are established to sell fraudulent products or services and/or to facilitate money-laundering.<sup>209</sup> This can involve establishing a salaried workforce with a well-defined division of labour and effectively mimicking the structures seen in lawful enterprises. The businesses can operate in plain sight, camouflaged within legitimate sectors, and in some cases may occupy grey areas that are on the peripheries of regulated business or commercial practices (see case study below).

Cybercrime has resulted in the diversification of the characteristics of fraud offenders. Technology is changing traditional notions of "street crime", with ever-more accessible technologies creating opportunities for criminals to engage in criminal activities such as phishing and online fraud.<sup>210</sup> Many occurrences of cyberfraud are perpetrated from outside legitimate or pseudo-legitimate business settings, often employing technology to impersonate an entity with whom a victim has a legitimate relationship.<sup>211</sup> Technology provides the gateway for involvement in these crimes, which can involve multiple forms of cybercrime (e.g. ransomware attacks), meaning that traditional notions of a fraudster may no longer represent offenders with the capacity to engage in a variety of cybercrimes for criminal gain.<sup>212</sup> This diversification is facilitated in part by the increasingly widespread availability of technological

<sup>&</sup>lt;sup>205</sup>One United Kingdom-based study found that the average age of organized fraudsters identified by United Kingdom law enforcement entities was 41 (May and Bhardwa, *Organised Crime Groups Involved in Fraud*, p. 113. See also Russell G. Smith, "Responding to organised crime through intervention in recruitment pathways", Trends and Issues in Crime and Criminal Justice Series, No. 473 (Canberra, Australian Institute of Criminology, 2014); and M. Vere van Koppen and others, "Criminal trajectories in organized crime", *The British Journal of Criminology*, vol. 50, No. 1 (January 2010)).

<sup>&</sup>lt;sup>206</sup>Van Koppen and others, "Criminal trajectories in organized crime".

<sup>&</sup>lt;sup>207</sup> UNODC, Organized Crime and Gender: Issues Relating to the United Nations Convention against Transnational Organized Crime (Vienna, 2022).

<sup>&</sup>lt;sup>208</sup> Anna Gekoski, Joanna Ruth Adler and Tim McSweeney, "Profiling the fraudster: findings from a rapid evidence assessment", *Global Crime*, vol. 23, No. 4 (2022); and David O. Friedrichs, *Trusted Criminals: White Collar Crime in Contemporary Society*, 4th ed. (Belmont, California, Wadsworth, 2010).

<sup>&</sup>lt;sup>209</sup> See, for example, Miramirkhani, Starov and Nikiforakis, "Dial one for scam"; Shover, Coffey and Sanders, "Dialing for dollars"; and UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia.

<sup>&</sup>lt;sup>210</sup> Leukfeldt, "Cybercrime and social ties"; and Robert A. Roks, Eric Rutger Leukfeldt and James A. Densley, "The hybridization of street offending in the Netherlands", *The British Journal of Criminology*, vol. 61, No. 4 (July 2021).

<sup>&</sup>lt;sup>211</sup> Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>212</sup>To illustrate, organized criminal groups engaged in cyberfraud in South-East Asia are reported to have diversified their business model to include the development of malware or malicious mobile or web applications and the provision of various cybercrimes as a service (UNODC, Regional Office for South-East Asia and the Pacific, *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia*).

knowledge resources through online criminal networks that can serve to expand the capabilities of an organized criminal group.<sup>213</sup>

This expansion of criminal opportunity is evident in many countries and regions. Studies have highlighted a phenomenon in which concentrations of specific fraud methodologies emanate from certain global regions. <sup>214</sup>Key examples include the concentration of romance, investment and other high-impact mass-marketing fraud perpetrated in West Africa that has strong associations with the local youth culture; <sup>215</sup> lottery fraud targeting the United States but emanating from Jamaica; <sup>216</sup> geographical "cybercrime hubs" in Eastern Europe that engage in fraud such as online auction fraud, wherein resources and learning are shared between those involved; <sup>217</sup> and scam compounds in South-East Asia that have industrialized processes for perpetrating romance and cryptocurrency investment fraud. <sup>218</sup>

### CASE STUDY: WHITE-COLLAR OFFENCES - INVESTMENT FRAUD



In the United Kingdom of Great Britain and Northern Ireland, criminals established a company for the purpose of defrauding pension holders of their savings. They acquired regulated status in order to appear as a legitimate provider and proceeded to market their financial services by making unsolicited calls to the public. They had a detailed knowledge and understanding of the United Kingdom pension sector, the relevant laws and regulations, investments and other financial instruments. Equipped with this knowledge, the criminals were able to exploit the public's considerable knowledge gaps. They employed a multilayered deception that first involved misleading victims about their tax liabilities to encourage them to release money. The money then passed through the hands of multiple co-offenders, who performed the role of financial intermediaries and charged inordinately high commission fees for processing the transfer of funds. The remaining money was then purported to have been invested in a legitimate but high-risk overseas company. The money was either lost after the investment failed or may never have been invested, but rather stolen by the criminals.

Source: Michael Skidmore, Protecting People's Pensions: Understanding and Preventing Scams (London, The Police Foundation, 2020), p. 15.

# Motivations of fraudsters

Technology has "democratized" fraud offending by opening up criminal opportunities to people in any social strata, including those from poor and disadvantaged backgrounds, who require neither specific occupational roles nor related skills and knowledge to be able to perpetrate organized fraud.<sup>219</sup> This criminality can be rooted in local subcultures, in which criminogenic attitudes, specialized knowledge

<sup>&</sup>lt;sup>213</sup>To illustrate, an organized criminal group in the United Kingdom had been involved in multiple categories of cyberfraud (identity fraud and business email compromise fraud). It also specialized in facilitating money-laundering and was involved in a ransomware attack against local businesses. The core offenders were not technically proficient but were able to access technical resources from other criminals, including online, such as in carding forums (Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending", p. 30).

<sup>&</sup>lt;sup>214</sup> INTERPOL, "INTERPOL global financial fraud assessment", p. 11.

<sup>&</sup>lt;sup>215</sup>Suleman Ibrahim, "Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals", *International Journal of Law, Crime and Justice*, vol. 47 (2016); and Monica T. Whitty, "419: it's just a game – pathways to cyber-fraud", *International Journal of Cyber Criminology*, vol. 12, No. 1 (January/June 2018).

<sup>&</sup>lt;sup>216</sup> Mortley, "A crime of opportunity".

<sup>&</sup>lt;sup>217</sup> Jonathan Lusthaus and Federico Varese, "Offline and local: the hidden face of cybercrime", *Policing: A Journal of Policy and Practice*, vol. 15, No. 1 (March 2017).

<sup>&</sup>lt;sup>218</sup> UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia.

<sup>&</sup>lt;sup>219</sup> Van der Geest, Weisburd and Blokland, "Developmental trajectories of offenders convicted of fraud"; and Wall, "Dis-organised crime".

and methodologies are propagated.<sup>220</sup> Cyberfraud in some contexts is afforded a social legitimacy, with particular rationalizations or attitudes shared by members of a community or group and successful fraudsters afforded a high social status.<sup>221</sup>

The obtainment of a criminal profit (financial or other material benefit) is the key motivation in fraud, as in virtually any acquisitive crime, which can be in response to an adverse financial situation, such as the absence of legitimate opportunities and deprivation. <sup>222</sup> In Nigeria, many cyberfraudsters are university students or graduates, commonly in their early to late 20s, with advanced knowledge of and skills in technology. <sup>223</sup> The gap between the growing levels of training and education and prospects in the legitimate economy can mean that individuals turn to illegitimate outlets such as cyberfraud to earn a living. <sup>224</sup> A similar pattern has been observed among scam compound recruits in South-East Asia: organized criminal groups recruit thousands of workers, many of whom are in their 20s and are university graduates with skills in ICT, social media, cryptocurrency and languages. <sup>225</sup> Many apply for these roles due to a lack of legitimate work opportunities, although, importantly, many are deceived into accepting what is presented as a legitimate position before being trafficked and coerced into perpetrating fraud. <sup>226</sup>

Criminals who become involved in organized criminal groups may make the conscious and intentional choice to become involved in fraud or may be recruited into an organized criminal group without having had any prior intention of becoming involved in organized crime.<sup>227</sup> For those who make an intentional choice, it can be for various reasons, such as being driven by greed when seeing an opportunity to make quick money, the influence of peers or associates in an existing organized criminal group or other group (offline or online), or financial need or difficulty.<sup>228</sup>

Among individuals with no prior intention of getting involved, many are recruited by organized criminal groups into peripheral, but important, enabling roles. This can include individuals recruited because they have specialist technical knowledge gained from working in a certain profession that can enable some part of the criminal process (e.g. solicitors or accountants), young professionals recruited into the "workforce" and members of the public enlisted into roles such as that of a money mule. Knowledge and complicity among these individuals can be variable and change over time: some have no awareness of the underlying fraudulent purpose of the activity, others are content to accept the money without asking too many questions and others come to knowingly participate in the crime.<sup>229</sup> Some co-offenders are exploited by the organized criminal group; they are often the most exposed to detection by law

<sup>&</sup>lt;sup>220</sup>See, for example, Alice Hutchings, "Crime from the keyboard: organised cybercrime, co-offending, initiation and knowledge transmission", *Crime, Law and Social Change*, vol. 62, No. 1 (August 2014); Lusthaus and Varese, "Offline and local"; Jegede Ajibade Ebenezer, "Cyber fraud, global trade and youth crime burden: Nigerian experience", *Afro Asian Journal of Social Sciences*, vol. 5, No. 4 (2014); and Ojedokun and Ilori, "Tools, techniques and underground networks".

<sup>&</sup>lt;sup>221</sup> Shover, Coffey and Sanders, "Dialing for dollars"; Whitty, "419: it's just a game"; and Oludayo Tade and Ibrahim Aliyu, "Social organization of Internet fraud among university undergraduates in Nigeria", *International Journal of Cyber Criminology*, vol. 5, No. 2 (July/December 2011).

<sup>&</sup>lt;sup>222</sup> Mortley, "A crime of opportunity".

<sup>&</sup>lt;sup>223</sup> Aransiola and Asindemade, "Understanding cybercrime perpetrators"; and Tade and Aliyu, "Social organization of internet fraud".

<sup>&</sup>lt;sup>224</sup> Akanle, Adesina and Akarah, "Towards human dignity and the internet"; and Suleman Lazarus and Geoffrey U. Okolorie, "The bifurcation of the Nigerian cybercriminals: narratives of the Economic and Financial Crimes Commission (EFCC) agents", *Telematics and Informatics*, vol. 40 (2019).

<sup>&</sup>lt;sup>225</sup>International Organization for Migration (IOM), Regional Office for Asia and the Pacific, "IOM's regional situation report on trafficking in persons into forced criminality in online scamming centre in Southeast Asia" (2024); and UNODC, Regional Office for South-East Asia and the Pacific, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*.

 $<sup>^{226}\,\</sup>mathrm{OHCHR},$  "Online scam operations and trafficking into forced criminality in Southeast Asia".

<sup>&</sup>lt;sup>227</sup> Smith, "Responding to organised crime through intervention in recruitment pathways".

<sup>&</sup>lt;sup>228</sup> See, for example, W. Steve Albrecht and Chad O. Albrecht, *Fraud Examination and Prevention* (Mason, Ohio, United States, Thompson South-Western, 2004); Hutchings, "Crime from the keyboard"; Yetunde O. Ogunleye, Usman A. Ojedokun and Adeyinka A. Aderinto, "Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in South-West Nigeria", *International Journal of Cyber Criminology*, vol. 13, No. 2 (July/December 2019); and May and Bhardwa, *Organised Crime Groups Impolación Estado* 

<sup>&</sup>lt;sup>229</sup>Shover, Coffey and Sanders, "Dialing for dollars"; Leukfeldt and Jansen, "Cyber criminal networks and money mules"; Levi, "Organized fraud and organizing frauds"; Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending"; and May and Bhardwa, *Organised Crime Groups Involved in Fraud*.

enforcement and thereby serve to put distance between the core criminals and the fraud, and in some cases receive little or no financial gain from their involvement.<sup>230</sup> In South-East Asia, a recent poignant example is the young people who accepted employment in scam compounds and were then subject to trafficking in persons and exploitation.<sup>231</sup>

A final point to consider is how fraudsters come to make the decision to target and steal money from victims, noting that some may otherwise not be involved in crime.<sup>232</sup> The process of rationalization to justify or neutralize the impact of the crime is important, because it can distort personal or group-based narratives on the gravity of the actions or even serve to legitimize them. Key examples include:

- The perception of an adversarial relationship with victims. A successful fraudster demonstrates
  the skill, mastery and power to control and manipulate the victims, who may be deemed
  unworthy (e.g. stupid or greedy) and blamed for falling for the fraud.<sup>233</sup>
- The perception of the crime as victimless or causing minimal harm. Such a perception may be
  present, for example, when fraudsters employ a method that involves the theft of small amounts
  of money from a high number of people or when the losses are experienced by corporations
  and companies rather than individuals.<sup>234</sup>
- The anonymous and remote nature of fraud, with impersonal exchanges that do not involve face-to-face contact with the victim. Offenders do not then directly observe the harm that is being caused, which can allow them to more readily neutralize their crimes. Moreover, in the context of cybercrime, the ability to remain physically invisible, to separate online action from offline identity and to perceive the online world as not being connected to "reality" disinhibits those who might otherwise not commit crime. As of the context of the cont
- The social and cultural influences that can serve to rationalize fraud. These can include sociopolitical narratives and perceptions of overseas victims: some fraudsters legitimize their actions on the basis of current or historic perceived social inequalities or injustices (e.g. "greedy westerners").<sup>237</sup> In some cultures, the perpetration of fraud can even be reinforced through local spiritual beliefs.<sup>238</sup>

Patterns in fraud offending have seen substantial changes in the past 10 to 20 years and continue to evolve at a fast pace. The research and knowledge base in the area are still developing and catching up with those changes. The characteristics of offenders and their pathways into organized fraud are highly variable, but there are patterns of behaviour that have begun to emerge in the different regions of the world and in the different commercial, financial and technological settings that foster criminal opportunity. Understanding who these criminals are and their routes into organized fraud is an important step in designing effective criminal justice and social policies to address these offending behaviours.

 $<sup>^{\</sup>rm 230}\,\rm Skidmore$  and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>231</sup> UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia.

<sup>&</sup>lt;sup>232</sup>For example, the "fraud triangle" is a prominent theory for explaining white-collar crime. It identifies three conditions for an offender to perpetrate fraud: (a) an incentive or pressure that provides a motive to commit fraud; (b) an opportunity for fraud to be perpetrated; and (c) an attitude that enables the individual to commit fraud or have the ability to rationalize the fraud (see Albrecht and Albrecht, *Fraud Examination and Prevention*).

<sup>&</sup>lt;sup>233</sup> Duffield and Grabosky, *The Psychology of Fraud*; and Shover, Coffey and Sanders, "Dialing for dollars".

<sup>&</sup>lt;sup>234</sup>Heath Copes and Lynne Vieraitis, "Identity theft: assessing offenders' motivations and strategies", in *In Their Own Words: Criminals on Crime*, 6th ed., Michael L. Birzer and Paul Cromwell, eds. (Oxford, Oxford University Press, 2014), pp. 124–139; Duffield and Grabosky, *The Psychology of Fraud*; and May and Bhardwa, *Organised Crime Groups Involved in Fraud*.

<sup>&</sup>lt;sup>235</sup> Duffield and Grabosky, *The Psychology of Fraud*; and Alice Hutchings, "Cybercrime trajectories: an integrated theory of initiation, maintenance and desistance", in *Crime Online: Correlates, Causes, and Context,* Thomas J. Holt, ed. (Durham, North Carolina, United States, Carolina Academic Press, 2010).

<sup>&</sup>lt;sup>236</sup> John Suler, "The online disinhibition effect", *Cyberpsychology and Behavior*, vol. 7, No. 3 (2004).

<sup>&</sup>lt;sup>237</sup> Mortley, "A crime of opportunity"; and Whitty, "419: it's just a game".

<sup>&</sup>lt;sup>238</sup> In Nigeria, some believe that the acquisition of wealth, whether by legitimate or illegitimate means, is rooted in the spiritual realm (Lazarus and Okolorie, "The bifurcation of the Nigerian cybercriminals").



# CHAPTER IV

# Cross-cutting facilitators of organized fraud

As highlighted in chapter II above, there is considerable diversity in the methods employed by different criminals to defraud victims; however, there are some commonalities in the behaviours and techniques used in different types of fraud. This is because, regardless of the specific fraudulent narrative that is presented to victims, many types of fraud need to accomplish the same overarching steps: establish communication with victims, employ methods of communication that facilitate deception, and access stolen funds without leaving an evidential trail.<sup>239</sup> Developing an understanding of the common elements of the legitimate and illegitimate economy that are exploited by fraudsters allows for the introduction of new strategies and interventions for preventing organized fraud. The present section contains a description of the following key underlying techniques, resources and technologies that have been identified in the policy and research literature: mass-marketing, identity theft, money-laundering and the enabling functions of technology (including emergent technologies such as artificial intelligence).

# Mass-marketing

The success of many types of consumer, employment and investment fraud is contingent on effective communications, using various techniques to persuade prospective investors. Such techniques include 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 thereof, which are deployed at different stages in the offence. For example, initial contact with a victim may be through a phishing website, which is followed by a subsequent sales call by telephone and then continued engagement through a fraudulent website (see case study below).

### 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 "lead lists" created by or bought from other legitimate or

<sup>&</sup>lt;sup>239</sup> The following three key stages in the process of cyberfraud were set out in one report: (a) the "inbound" communication route; (b) the "interaction" with the victim; and (c) the "cashing out" (United Kingdom, House of Lords, Fraud Act 2006 and Digital Fraud Committee, *Fighting Fraud: Breaking the Chain*, Report of Session 2022–23, House of Lords Paper, No. 87 (London, 2022)).

illegitimate actors who compile and sell this personal information on consumers.<sup>240</sup> In some cases, these lists include individuals known to have been previously defrauded and thus to be potentially vulnerable to similar approaches; this problem is particularly acute for older victims in vulnerable contexts.<sup>241</sup> Call centres can be managed directly by the offenders running the fraudulent scheme or contracted out to specialists who 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 such activities.<sup>242</sup>

## Online communications

There has been a substantial rise in fraud for which the initial contact with victims is established through online communications such as social media and fraudulent websites and applications.<sup>243</sup> The capacity to engage in large-scale and targeted marketing is greatly enhanced by the accessibility of digital technologies and large data sets on consumers. For example, websites and online advertisements can be used to collect data on individuals with an interest in the product or service that is being offered, providing a means to target subsequent communication.<sup>244</sup>

## Other communications

Other methods include fraud marketed through the postal service or in person.<sup>245</sup> Some categories, such as investment fraud, commonly involve large sums of money that are highly significant to victims, and face-to-face contact remains important in some cases to achieve sufficient levels of trust to secure an investment. Some fraudsters target victims with whom they have existing social or business connections to exploit a trust relationship that already exists.<sup>246</sup>

# Identity theft

In an information society where digital transactions increasingly take the place of face-to-face interactions, the instruments and mechanisms for verifying identification are critical.<sup>247</sup> Identity theft and identity fraud represent two discrete activities: identity theft relates to the processes for accessing and stealing the data, and identity fraud involves the application of the stolen data to deceive victims and fraudulently access funds or other material benefits. ICT and big data facilitate the transfer of information on an unprecedented scale, and this capability is exploited by criminals. Technology acts as a

<sup>&</sup>lt;sup>240</sup> Shover, Coffey and Sanders, "Dialing for dollars"; Levi, "Organized fraud and organizing frauds"; and Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>241</sup> Age UK, Only the Tip of the Iceberg: Fraud against Older People – Evidence Review (London, 2015); and Mark Button and others, "Fear and phoning: telephones, fraud, and older adults in the UK", International Review of Victimology (2024).

<sup>&</sup>lt;sup>242</sup> Shover, Coffey and Sanders, "Dialing for dollars".

<sup>&</sup>lt;sup>243</sup>See, for example, United States, Federal Bureau of Investigation, "The FBI warns of a spike in cryptocurrency investment schemes", 14 March 2023; and United Kingdom, Financial Conduct Authority, "FCA warns of increased risk of online investment fraud, as investors lose £87k a day to binary options scams", 12 April 2024.

<sup>&</sup>lt;sup>244</sup> See, for example, Liu and others, "Understanding, measuring, and detecting".

<sup>&</sup>lt;sup>245</sup> See, for example, DeLiema and Langton, "Older victims of mass marketing scams"; and Phillips, "From 'rogue traders' to organized crime groups".

<sup>&</sup>lt;sup>246</sup> Frank S. Perri and Richard G. Brody, "The optics of fraud: affiliations that enhance offender credibility", *Journal of Financial Crime*, vol. 19, No. 3 (2012).

<sup>&</sup>lt;sup>247</sup> Bert-Jaap Koops and others, "A typology of identity-related crime", Information Communication and Society, vol. 12, No. 1 (2009).

force multiplier for identity theft, by increasing the capacity to quickly access high volumes of personal information at the global level.<sup>248</sup> Methods for perpetrating identity theft include:

- Use of social engineering techniques. These include phishing, smishing and spear phishing attacks<sup>249</sup> that use targeted communications to pressure a recipient into making a quick decision to respond (e.g. a purported threat to the security of an account).<sup>250</sup> Phishing campaigns are a tactic used to trick individuals into divulging personal information as well as a vehicle to initiate malware-based attacks on electronic devices.
- Collection of open-source data. Criminals can exploit the data that are posted by users on social media platforms. Large volumes of data can be harvested using automated software, or a fraudster may profile an intended victim to facilitate the deception.
- Intrusion into (or infection of) a computer or device. Fraudsters infect a victim's computer with malware that enables them to monitor activity and harvest personal details and account information. In one method, the Internet browser is manipulated so that, when a person attempts to access a legitimate website, they are redirected to a spoofed website that allows offenders to collect account information.<sup>251</sup> Botnets and other surveillance software increase attackers' capacity to infect a high volume of computers with malware that can be controlled remotely by the attacker and used to search for personal information, including information for accessing accounts.
- Digital skimming. The use of malware to infiltrate legitimate websites such as those of online retailers is known as digital skimming. Payment information (e.g. credit card credentials) may be taken directly from the legitimate payment form, or a buyer may be redirected to a fake checkout web page to enter their details.<sup>252</sup>
- Data breach through hacking or other means of intrusion into the ICT systems of organizations that store large amounts of personal data.<sup>253</sup> Analysis of data breaches from 2005 to 2018 revealed 9,000 data breaches that had led to the loss of 11.5 billion individual records, with hacking playing an increasingly central role.<sup>254</sup> The large-scale theft of personal data can enable various types of fraud, although the proportion of the data that is used in this way is not known.

Identity theft is a vital precursor event in many types of fraud and a key enabler of others. For example, it facilitates identity fraud, mass-marketing and the opening of bank accounts to facilitate money-laundering. Identity theft and the ensuing fraudulent activity are not necessarily perpetrated as part of a single criminal process, with online criminal markets such as carding forums providing cybercriminals with convenient and efficient channels to supply stolen data to would-be fraudsters.<sup>255</sup>

<sup>&</sup>lt;sup>248</sup> David S. Wall, "Policing identity crimes", Policing and Society: An International Journal of Research and Policy, vol. 23, No. 4 (2013).

<sup>&</sup>lt;sup>249</sup> Phishing is a form of communication that appears to come from a reputable or trustworthy source that is intended to solicit personal information or payment, or may contain attachments that install malware if opened; smishing is a form of phishing that is received by text message or messaging applications; spear phishing is a more targeted attack in which the perpetrators use information about the recipient to make the message more realistic and persuasive. See, for example, Europol, "Online fraud schemes"; and Europol, European Cybercrime Centre, "Spear phishing: a law enforcement and cross-industry perspective" (The Hague, 2019).

<sup>&</sup>lt;sup>250</sup> Zainab Alkhalil and others, "Phishing attacks: a recent comprehensive study and a new anatomy", Frontiers in Computer Science, vol. 3, art. No. 563060 (March 2021).

<sup>&</sup>lt;sup>251</sup> Wall, "Policing identity crimes".

<sup>&</sup>lt;sup>252</sup> Europol, "Online fraud schemes".

<sup>&</sup>lt;sup>253</sup> Spencer Wheatley, Thomas Maillart and Didier Sornette, "The extreme risk of personal data breaches and the erosion of privacy", *The European Physical Journal B*, vol. 89, art. No. 7 (January 2016).

<sup>&</sup>lt;sup>254</sup> Hicham Hammouchi and others, "Digging deeper into data breaches: an exploratory data analysis of hacking breaches over time", *Procedia Computer Science*, vol. 151 (2019).

<sup>&</sup>lt;sup>255</sup> Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (Luxembourg, Publications Office of the European Union).

### CASE STUDY: DATA BREACH



An organized criminal group hacked the computer networks of multiple corporations, resulting in a large-scale data breach in which 160 million credit card numbers were stolen. The group used malware to attack and infiltrate the corporate systems. They concealed this activity by deploying malware that could not be detected by the anti-virus software and leasing servers that were inaccessible to law enforcement ("bullet-proof hosts"). The stolen credit card numbers and associated personal information were sold in batches. The buyers encoded the stolen data onto the magnetic strips of plastic bank cards and used them to withdraw cash from accounts or make unauthorized purchases.

Source: United States v. Drinkman, Kalinin, Kotov, Rytikov, Smilianets, available from the Sharing Electronic Resources and Laws on Crime (SHERLOC) knowledge management portal.

# Money-laundering

For any perpetrator of fraud, a key consideration is how to disguise the illegal origins of the stolen funds. Money-laundering is the acquisition, possession, use, concealment, conversion or transfer of any property, knowing that such property is the proceeds of crime.<sup>256</sup>

Organized criminal groups require processes for accessing stolen funds without triggering controls in the finance or other sectors or leaving a financial trail that can be traced by law enforcement.<sup>257</sup> In addition to wire transfers through traditional banking and fintech companies, the proceeds of fraud, like any other crime generating illicit gain, can be laundered through money mules and shell companies,<sup>258</sup> by purchasing real estate or high-value goods such as cars or by using currency exchange bureaux, casinos, front companies or underground banking services such as hawala transactions.<sup>259</sup>

The globalization of trade and finance, facilitated by growth, diversification and technological advancements in the finance sector, has introduced new and evolving channels to exploit for criminals seeking to launder the proceeds of crime. <sup>260</sup> Criminals continuously adapt to and exploit new and evolving channels that facilitate the quick movement of funds and capital across national borders. <sup>261</sup> Examples include criminals who use trade-based money-laundering as a method, namely "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins". Trade-based money-laundering is typically effected through the misinvoicing of international trade transactions. By fraudulently misreporting the price, quantity or quality of goods, criminals can quickly move substantial amounts of money or value from one jurisdiction to another. <sup>262</sup>

<sup>&</sup>lt;sup>256</sup> Organized Crime Convention, art. 6. See also Benjámin Villányi, "Money laundering: history, regulations, and techniques", *Criminology and Criminal Justice*, 26 April 2021.

<sup>&</sup>lt;sup>257</sup> INTERPOL, "INTERPOL global financial fraud assessment", p. 18.

<sup>&</sup>lt;sup>258</sup> Financial Action Task Force, INTERPOL and Egmont Group of Financial Intelligence Units, *Illicit Financial Flows from Cyber-Enabled Fraud* (Paris, 2023).

<sup>&</sup>lt;sup>259</sup> Nigerian Financial Intelligence Unit, "Nigeria releases money-laundering typologies through fraud report"; and UNODC, Regional Office for South-East Asia and the Pacific, Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia

<sup>&</sup>lt;sup>260</sup> Emilia A. Isolauri and Irfan Ameer, "Money laundering as a transnational business phenomenon: a systematic review and future agenda", *Critical Perspectives on International Business*, vol. 19, No. 3 (April 2023); Europol, *The Other Side of the Coin: An Analysis of Financial and Economic Crime*, European Financial and Economic Crime Threat Assessment 2023 (Luxembourg, Publications Office of the European Union, 2023); and Pierre Bardin and others, "Money laundering poses a risk to financial sector stability", International Monetary Fund Blog, 4 September 2023.

<sup>&</sup>lt;sup>261</sup> Isolauri and Ameer, "Money laundering as a transnational business phenomenon".

<sup>&</sup>lt;sup>262</sup> Financial Action Task Force, "Trade based money laundering" (Paris, 2006).

Complex and cross-border business arrangements and transactions create considerable challenges for law enforcement entities and industry to trace the origins of goods and distinguish illegitimate from legitimate financial and commercial activity.<sup>263</sup> Effective international cooperation may be required to trace stolen funds laundered in this way.

Cryptocurrencies are increasingly used to launder the proceeds of serious and organized crime, with fraud being one of the most common predicate offences for money laundered in this way. <sup>264</sup> The purchase of cryptocurrencies and their use to transfer funds help provide anonymity and facilitate the international transfer of funds in a way that obfuscates the financial trail and conceals the criminal origins of the money. This commonly involves transferring cryptocurrency and other digital assets across different blockchain networks (or "coins") to obscure the trail, before cashing out the money by converting it back into a fiat currency. <sup>265</sup> This helps bypass stringent anti-money-laundering controls that are implemented by traditional financial institutions. There are challenges to imposing robust regulation, particularly due to the growth in decentralized finance. <sup>266</sup> These services facilitate the transfer of cryptocurrencies into other virtual assets without the need for a centralized intermediary that could identify the suspicious activity and bring it to the attention of the authorities. <sup>267</sup> Cryptocurrency exchange sites are numerous and can be used to transfer virtual assets across platforms or convert cryptocurrency into fiat currency. Some such sites are unlicensed or are located in countries that have little regulation in place and/or that choose to implement few controls to prevent money-laundering (see case study below). <sup>268</sup>

Money-laundering capabilities and resources are highly valued by criminals engaged in organized fraud, and the processes of money-laundering can represent a key element of organization that drives the formation of the organized criminal group. <sup>269</sup> Professional enablers play a key role in some fraud schemes, particularly those that exploit legal business structures to launder the criminal proceeds. <sup>270</sup> Studies have highlighted the prominent role of solicitors, accountants, financial advisers, bank managers and mortgage brokers in facilitating the laundering of the proceeds of fraud. <sup>271</sup> This includes the use of professional money-laundering networks by fraudsters, <sup>272</sup> professionals who are corrupted and those who unwittingly facilitate money-laundering, sometimes by neglecting due diligence procedures. It is important to conduct stand-alone money-laundering investigations into those professionals who offer services to multiple organized criminal groups for a fee.

Some organized criminal groups enlist criminals with specialized money-laundering capabilities, including those who advertise their services on online criminal markets. This can be especially valuable in facilitating transnational fraud, where co-offenders in the target country (i.e. where the victims are

<sup>&</sup>lt;sup>263</sup>See, for example, James Treadwell, "From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace", *Criminology and Criminal Justice*, vol. 12, No. 2 (April 2012).

<sup>&</sup>lt;sup>264</sup> This is the most prevalent modus operandi for fraudsters operating in Europe (INTERPOL, "INTERPOL global financial fraud assessment", p. 17; and Europol, *Cryptocurrencies: Tracing the Evolution of Criminal Finances*, Europol Spotlight Report Series (Luxembourg, Publications Office of the European Union, 2021).

<sup>&</sup>lt;sup>265</sup> Vladlena Benson, Umut Turksen and Bogdan Adamyk, "Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities", *Journal of Financial Regulation and Compliance*, vol. 32, No. 1 (January 2024).

<sup>&</sup>lt;sup>266</sup> Decentralized finance is a system of financial products and services that uses smart contracts on blockchains to manage a financial transaction between two parties. This technology enables automated exchanges in which people can trade directly with one another, removing the requirement for a centralized institution or third party to be involved (e.g. a bank or cryptocurrency provider). See, for example, Organisation for Economic Co-operation and Development, *Why Decentralised Finance (DeFi) Matters and the Policy Implications* (2022).

<sup>&</sup>lt;sup>267</sup> Benson, Turksen and Adamyk, "Dark side of decentralised finance".

<sup>&</sup>lt;sup>268</sup> See, for example, United States Attorney's Office, Southern District of New York, "Tornado cash founders charged with money laundering and sanctions violations", press release, 23 August 2023.

<sup>&</sup>lt;sup>269</sup> Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

<sup>&</sup>lt;sup>270</sup> Europol, *The Other Side of the Coin*.

<sup>&</sup>lt;sup>271</sup> Michael Levi, "Making sense of professional enablers' involvement in laundering organized crime proceeds and of their regulation", *Trends in Organized Crime*, vol. 24, No. 1 (March 2021); and May and Bhardwa, *Organised Criminal Groups Involved in Fraud*.

<sup>&</sup>lt;sup>272</sup> Financial Action Task Force, INTERPOL and Egmont Group of Financial Intelligence Units, *Illicit Financial Flows from Cyber-Enabled Fraud*, p. 15.

located) receive and transfer the stolen funds overseas.<sup>273</sup> The recruitment of money mules involves paying individuals a fee to receive illicit funds into their own bank accounts and then wire the money to an account controlled by the offender. This serves to disperse the stolen funds and thereby reduce the risk of detection by a financial service provider. Fraudsters employ various methods to recruit money mules, including posting advertisements online and recruiting from within the local community.<sup>274</sup> They may be recruited from within an existing social network or from among groups who are in financial need (e.g. children and youth or university students) or in vulnerable contexts who might also be a target for fraud.<sup>275</sup>

### CASE STUDY: FACILITATION OF MONEY-LAUNDERING



A virtual currency exchange registered in Costa Rica was alleged to have facilitated the laundering of \$6 billion. For a small fee, users were able to deposit and convert fiat currency into digital currency and transfer this money to other users. The company recorded minimal data on the users of the service and the authorities believed that the company was designed with the intention of concealing the identities of its users and rendering them untraceable. The service was utilized by cybercriminals engaged in a range of predicate crimes, including credit card fraud and identity theft.

Source: Yongyu Zeng and David Buil-Gil, "Organizational and organized cybercrime", in Oxford Research Encyclopedia of Criminology and Criminal Justice, H. Pontell, ed. (Oxford, Oxford University Press, 2023).

### CASE STUDY: ROMANCE FRAUD



In Nigeria, two brothers were identified as having been engaged in romance fraud that likely targeted a multitude of victims. One of the brothers facilitated access to multiple foreign bank accounts, several of which were registered to companies that transpired to be front companies. The companies and accounts were established in collaboration with the manager of a local bank and a co-offender located in China. Significant sums were deposited into those company accounts, with one company recorded as having a multimillion dollar turnover. The fraudsters in Nigeria sold cryptocurrency to the co-offender in China, who then made the payments into the company accounts.

Source: Nigerian Financial Intelligence Unit, "Nigeria releases money-laundering typologies through fraud report", 12 August 2023.

<sup>&</sup>lt;sup>273</sup> Manny Aston and others, "A preliminary profiling of internet money mules: an Australian perspective", in *Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (2009); Conradt, "Online auction fraud and criminological theories"; and Whittaker and Button, "Understanding pet scams".

<sup>&</sup>lt;sup>274</sup> Leukfeldt and Jansen, "Cyber criminal networks and money mules"; and Soudijn and Zegers, "Cybercrime and virtual offender convergence settings".

<sup>&</sup>lt;sup>275</sup> Skidmore and Aitkenhead, "Understanding the characteristics of serious fraud offending".

# **Enabling technology**

# Technology to conceal criminality

The increased availability of encryption tools plays an important role in enabling cybercrimes such as fraud, including the use of virtual private networks, end-to-end encryption for communications, the dark web and bullet-proof hosting services. The Many of these technologies are legal and legitimately available (e.g. virtual private network services), although some are designed and supplied by criminals. The While some of these tools may have legitimate uses by the general population, they can also help to conceal identities and facilitate secure communication and exchanges between criminals online. The dark web is an encrypted layer of the Internet that allows users to remain hidden and untraceable. Cryptocurrencies are a preferred method of payment in the exchange of illicit goods and services on the dark web, which adds another layer of obfuscation to make them more difficult to trace. To illustrate, a large criminal marketplace had operated using a hidden service on the Tor network which concealed the identities of users and server locations. At one time, the site had 200,000 users and, since its establishment, transactions on the market were estimated to total \$1 billion; the transactions commonly involved bitcoin or other cryptocurrencies. A range of criminal tools and resources were listed on the site, including fraudulent identity documents and access devices, counterfeit goods and other fraudulent services.

# Technology to facilitate deception

Modern technology has industrialized fraud methodologies that have long been in existence.<sup>281</sup> Digital environments enhance the capabilities to communicate with victims, engage in fraudulent commercial and financial transactions and exploit large data sets. Furthermore, new technologies developed by legitimate and illegitimate actors have automated otherwise laborious and costly processes. Examples include the use of bots to make thousands of clicks on a website in order to manipulate search engine rankings (i.e. click fraud), and cheap and readily available SIM farm devices that hold multiple SIM cards to make fraudulent calls or send text messages in high volumes to potential victims.

A key factor in the evolution of fraud methodologies is the requirement for offenders to continuously adapt to the countervailing security measures that are introduced by the State or industry.<sup>282</sup> One example is the rise in card-not-present fraud, which emerged in response to the introduction of chip-and-PIN to increase card security.<sup>283</sup> More recent examples include the emergence of digital fingerprint theft from compromised devices to counteract the increased use of biometric data for authenticating identity and accessing accounts.<sup>284</sup> Artificial intelligence technologies have the potential to heighten

<sup>&</sup>lt;sup>276</sup> Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*; Europol, European Cybercrime Centre and European Union Agency for Criminal Justice Cooperation (Eurojust), "First report of the observatory function on encryption" (The Hague, 2019); Europol and Eurojust Public Information, "Common challenges in combating cybercrime" (2019); and Annamaria Szakonyi, Brian Leonard and Maurice Dawson, "Dark web: a breeding ground for ID theft and financial crimes", in *Handbook of Research on Theory and Practice of Financial Crimes*, Abdul Rafay, ed. (Hershey, Pennsylvania, United States, IGI Global, 2021).

<sup>&</sup>lt;sup>277</sup> Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023.

 $<sup>^{\</sup>rm 278}$  Szakonyi, Leonard and Dawson, "Dark web: a breeding ground for ID theft and financial crimes".

<sup>&</sup>lt;sup>279</sup> Tor is a browser used to access the dark web.

<sup>&</sup>lt;sup>280</sup> Europol, "Massive blow to criminal dark web activities after globally coordinated operation", 20 July 2017.

<sup>&</sup>lt;sup>281</sup>Button and Cross, Cyber Frauds, Scams and Their Victims.

<sup>&</sup>lt;sup>282</sup> Albanese, "Fraud".

<sup>&</sup>lt;sup>283</sup> Michael Levi, "Organising and controlling payment card fraud: fraudsters and their operational environment", *Security Journal*, vol. 16, No. 2 (April 2003).

<sup>&</sup>lt;sup>284</sup> Europol, "Online fraud schemes".

this adversarial environment by increasing the capabilities of criminals to perpetrate fraud, while also offering the potential for organizations to improve their cyberdefences.<sup>285</sup>

The developments in artificial intelligence, in particular generative artificial intelligence, which is capable of generating content that mimics human characteristics, are likely to play a key role in shaping fraud in the future. It is predicted that the capabilities of fraudsters will be enhanced in two ways: (a) amplifying the reach and volume of offending by facilitating the production of larger amounts of fraudulent content at greater speed; and (b) refining the existing methods of social engineering by producing more sophisticated, convincing and personalized content.<sup>286</sup>

The use of artificial intelligence has been noted in the following aspects of fraud:

- Preparing and targeting. Artificial intelligence technologies increase the capacity of offenders to process and review large volumes of data to target vulnerabilities and quickly process stolen data to extract more value.<sup>287</sup> Generative artificial intelligence will be able to design and produce more refined and tailored content at speed, such as text, images and documents to facilitate fraud.<sup>288</sup> FraudGPT, a generative artificial intelligence tool designed to facilitate cybercrime, is capable of automating a variety of tasks, including the creation of fraudulent materials such as emails.<sup>289</sup>
- Social engineering. Voice clones and deep-fake technologies provide offenders with enhanced capability to impersonate individuals or entities trusted by victims to promote fraudulent products or services.
- Evading detection. The increased use of artificial intelligence technology in the perpetration
  of fraud has the potential to augment anonymity and further obfuscate the trail back to the
  criminals who are responsible.<sup>290</sup>

It has been noted that fraudsters are avid customers of cybercrime as a service, making use of tools and/or data on offer.<sup>291</sup> It is anticipated that the greater legitimate availability of artificial intelligence technology and the increased supply of artificial intelligence-enabled cybertools in underground criminal markets will serve to improve the capabilities of would-be fraud offenders who are less technically skilled.<sup>292</sup> The consequence is the lowering of the barriers to entry for engaging in organized fraud.

In the present section, some of the techniques and resources that play a key underlying role in facilitating the many variants of organized fraud have been highlighted. The diverse range of channels through which fraudsters communicate with victims and employ deception, and the range of techniques used to frustrate the efforts of law enforcement and avert the risk of detection and punishment, have also been

<sup>&</sup>lt;sup>285</sup> Borja Álvarez Martínez and others, "Mapping the state of the art: artificial intelligence for decision-making in financial crime", in *Cybersecurity for Decision Makers*, Narashima Rao Yajihala and Kenneth David Strang, eds. (Boca Raton, Florida, United States, CRC Press, 2023). https://www.routledge.com/Cybersecurity-for-Decision-Makers/Vajjhala-Strang/p/book/9781032334974?srsltid=AfmBOoqL0-ovS3IO4TG\_gXX5erTA9rOcLN0rjwAxlbsccdVeH4w-ICPo

 $<sup>^{286}</sup> Price waterhouse Coopers\ and\ Stop\ Scams\ UK,\ "Impact\ of\ artificial\ intelligence\ on\ fraud\ and\ scams"\ (2023),\ p.\ 9.$ 

<sup>&</sup>lt;sup>287</sup> United Kingdom, National Cyber Security Centre, "The near-term impact of AI on the cyber threat" (2024).

<sup>&</sup>lt;sup>288</sup> PricewaterhouseCoopers and Stop Scams UK, "Impact of artificial intelligence on fraud and scams".

<sup>&</sup>lt;sup>289</sup> Falade, "Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks", *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 9, No. 5 (September/October 2023).

<sup>&</sup>lt;sup>290</sup> See www.acfeinsights.com/acfe-insights/2023/1/6/ai-and-fraud.

<sup>&</sup>lt;sup>291</sup> Europol, "Online fraud schemes".

<sup>&</sup>lt;sup>292</sup> United Kingdom, National Cyber Security Centre, "The near-term impact of AI on the cyber threat".

highlighted. These methods continuously evolve, often in conjunction with legitimate global changes in communications, finance, commerce and technology. It is important that Member States, in partner-ship with key industries such as the finance and technology sectors, identify and track the underlying methods adopted by fraudsters to deliver more effective strategic responses to prevent these crimes.



# CHAPTER V

# Tackling organized fraud

Organized fraud is perpetrated in high volumes and penetrates many commercial and financial sectors. For the perpetrators, the rewards are high and the barriers and risks are low. A comprehensive response includes crime prevention strategies and adequate laws to close off the abundant criminal opportunities for perpetrating these crimes, in conjunction with robust law enforcement to target and deter offenders. More effective controls are needed to address the technical vulnerabilities in infrastructure and systems and to provide education and promote awareness in the public and business sectors to help defend against fraud. Strategic responses should consider the following principles:<sup>293</sup>

- Prevent organized crime from (re)infiltrating communities, the economy and political institutions
- Pursue organized criminal groups and their illicit gains, thereby increasing their operational costs and risks
- Protect vulnerable persons and victims from (further) harm
- Promote partnerships and cooperation at all levels, including across international borders a whole-of-society approach

Strategies against organized crime need to account for the complexities of the organized fraud problem, especially as it is transnational, exploits global technologies and systems and continuously adapts to changes in commercial and financial systems. Change is contingent on policies that take a multipronged approach that coordinates responses across government departments and agencies, key sectors in private industry and civil society. There is also a need for greater international collaboration to understand and address organized fraud that crosses borders.

Such whole-of-society comprehensive strategies against organized crime are particularly important in contexts where organized criminal groups are increasingly poly-criminal,<sup>294</sup> engaging in various forms of organized crime, including organized fraud. Isolated strategies or responses focused on one area only, such as securing criminal justice outcomes, would not sufficiently address the multidimensional character of organized criminal groups involved in the commission of multiple offences. Moreover, a lack of coordination between responses to different crime types may create loopholes, duplicate efforts and inadequately use restricted resources. Regional and national strategies against organized crime

<sup>&</sup>lt;sup>293</sup> UNODC, "Organized crime strategy toolkit for developing high-impact strategies" (Vienna, 2021).

<sup>&</sup>lt;sup>294</sup> See, for example, UNODC, Regional Office for South-East Asia and the Pacific, *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia*; and UNODC Research and Trend Analysis Branch and UNODC Regional Office for West and Central Africa, "Impact of transnational organized crime on stability and development in the Sahel" (Vienna, 2024). <a href="https://www.unodc.org/documents/data-and-analysis/tocta\_sahel/TOCTA\_Sahel\_Transversal\_2024.pdf">https://www.unodc.org/documents/data-and-analysis/tocta\_sahel/TOCTA\_Sahel\_Transversal\_2024.pdf</a>

structured around the four pillars mentioned above (prevent, pursue, protect and promote) can serve as an umbrella framework to be complemented by tailored crime-specific responses, such as action plans, coordination centres and task forces against organized fraud.

# CHECKLIST FOR REVIEWING STRATEGIES AND CRAFTING ACTION PLANS AGAINST FRAUD

PREVENT organized fraud	
	Strategic analysis to identify and assess the economic, cultural, social and institutional root causes of marginalization and vulnerability that create the pathways into involvement in fraud
	Responses to divert or deter groups vulnerable to being recruited or otherwise drawn into fraud. This includes addressing those in key sectors and professions who are vulnerable to corruption and taking measures to encourage reporting and protect victims, witnesses, informants and whistle-blowers
	Measures to challenge the narratives of organized criminal groups recruiting individuals to commit fraud
PURSUE organized criminal groups	
	Legislation in place for the criminalization of fraud, including, where appropriate, making fraud a serious crime, in accordance with article 2 (b) of the Organized Crime Convention. Penalties should be dissuasive, proportionate, clear and certain, avoiding any violation of human or constitutional rights
	Law enforcement agencies and the judiciary equipped with the technical skills to effectively investigate organized fraud, including financial investigation, cybercrime investigation, digital forensics and relevant special investigative techniques, and to identify, trace, freeze, seize and confiscate proceeds of crime and other assets
	Database systems to aggregate and analyse national law enforcement data to facilitate the identification of organized criminal groups and inform the strategic and tactical responses to organized fraud
PROTECT persons affected by organized fraud	
	Campaigns to raise awareness among the public and business community to foster secure behaviours and protect against becoming a victim of fraud
	Measures for identifying and supporting victims who are vulnerable and at risk of being repeatedly defrauded and serious harm
PROMOTE partnerships and cooperation	
	Whole-of-society approach to preventing and combating fraud, including the private sector, civil society, academia and education actors, as appropriate
	Clear reporting channels for the public and business community to report fraud to law enforcement entities and access the support needed
	Legislative and other measures to guide information-sharing between the State and the private sector, including businesses in key industries such as finance and technology
	Measures to drive strategic engagement with business and industry bodies in key private sectors, identify systemic weaknesses and vulnerabilities and coordinate effective strategic responses to prevent fraud
	Frameworks to foster international cooperation in criminal matters, including through mutual legal assistance and joint investigation teams

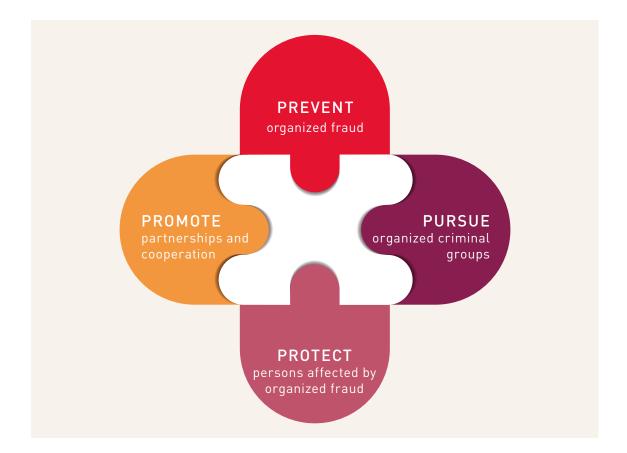


FIGURE. FOUR STRATEGIC PILLARS FOR TACKLING ORGANIZED FRAUD

# Prevention of organized fraud

Prevention campaigns and interventions can be targeted to deter individuals from pathways into organized fraud offending. The research is limited but, in certain subcultures, the perpetrators of fraud and cybercrime are afforded social legitimacy. Individuals in these communities and networks can adopt various narratives to rationalize their offending behaviour; examples include a view that victims are getting what they deserve (e.g. they are greedy) or attitudes that minimize the crimes and harms that are caused by the fraud.<sup>295</sup> Moreover, fraud can offer the offenders a means to achieve material success that would otherwise be unobtainable, particularly in regions where poverty is high and legitimate prospects low. In some cases, fraudsters gain local prominence and make public displays of wealth, which makes them aspirational figures for young people. Some young people engage in cybercrime without being aware that they are committing a crime or causing harm.<sup>296</sup> Such crimes may amount to low-level fraud but bring the risk that the offenders will be lured in by the prospect of criminal profits and escalate to organized fraud. The patterns and pathways into organized fraud need to be understood within the local social, economic and political contexts, and interventions need to be targeted to address the root causes of fraud offending.<sup>297</sup>

<sup>&</sup>lt;sup>295</sup> See, for example, Shover, Coffey and Sanders, "Dialing for dollars"; and Whitty, "419: it's just a game".

<sup>&</sup>lt;sup>296</sup> Mary Aiken, Julia Davidson and Philipp Amann, "Youth pathways into cybercrime" (2016).

<sup>&</sup>lt;sup>297</sup> See, for example, Lorenzo Pasculli, "Coronavirus and fraud in the UK: from the responsibilisation of the civil society to the deresponsibilisation of the state", *Coventry Law Journal*, vol. 25, No. 2 (December 2020).

Organized criminal groups involved in fraud incorporate loose associations with individuals who are vital for facilitating the crime but adopt a peripheral role in the fraudulent scheme. This includes individuals in professional occupations who facilitate fraud (e.g. law and finance professionals) and members of the public who provide use of their accounts for a fee (i.e. money mules). For these co-offenders, the levels of complicity and culpability can be ambiguous, with some content to take the money without asking too many questions about the underlying crimes. Public information campaigns targeted at such at-risk groups to highlight the seriousness of the crime and the risk that they will receive criminal justice sanctions may serve to increase awareness and divert and deter individuals from engaging in these crimes.

## CASE STUDY: DIVERTING YOUNG PEOPLE FROM CYBERCRIME



In response to an increase in the volume of young people entering the criminal justice system for hacking offences, the Kingdom of the Netherlands established the HACK\_Right rehabilitation programme for first-time offenders aged between 12 and 30. The programme serves to raise awareness of the law, the consequences of engaging in hacking and the impact on victims. The aim is to divert people away from cybercrime and other potentially more serious crimes (such as organized fraud) and redirect those skills into legitimate activities.

Source: J.A.M. Schiks, Susanne van 't Hoff-de Goede and E. Rutger Leukfeldt, "An alternative intervention for juvenile hackers? A qualitative evaluation of the Hack\_Right intervention", Journal of Crime and Justice (2023).

# Pursuit of organized criminal groups

## Legislation

The adoption of clear and robust legal frameworks is important for assessing and tackling fraud, so as to ensure that practitioners can confidently identify the presence of organized crime and assign the commensurate resources and interventions. Furthermore, international cooperation is contingent on having a clear and common understanding across the different legal jurisdictions of what constitutes organized fraud, guided by the provisions of the Organized Crime Convention.

Some Member States have addressed fraud-related offences in specialized legislation, whereas others have incorporated such offences into existing criminal codes. Fraud can also be addressed in a multitude of laws, creating multiple definitions. There is a need for legal frameworks to provide sufficient:

- Clarity, to facilitate practitioner understanding to ensure the effective application of the law and a clear delineation of lawful and unlawful behaviours
- Coverage, which should be comprehensive and flexible enough to capture the diversity of
  methods used to perpetrate fraud, including emerging and future methods such as those that
  exploit new technologies<sup>298</sup>

<sup>&</sup>lt;sup>298</sup> See, for example, Ben Summers, "The Fraud Act 2006: has it had any impact?", Amicus Curiae, No. 75 (2008).

Some countries have adopted highly specified and prescriptive legal definitions of fraud that enumerate the various products, services or techniques that constitute fraudulent activity in law, for example, the use of a victim's personal information, impersonating an authority or creating a false hope of winning something. Others employ broad legal definitions that can be applied to a range of scenarios or criminal contexts (see chap. I above). Fraud is highly diverse in the methods employed by the perpetrators and the impact on victims or more widely. Thus, countries' sentencing frameworks vary, including the presence of aggravating and mitigating factors, which can refer to the experience of the victim, the characteristics of the fraudsters and the perpetration of certain categories of fraud.<sup>299</sup>

The combination of aggravating factors included in the legislation can determine the types of fraud offending and the maximum sentence, which can vary among States. A victim-centric perspective has been adopted in some legal frameworks, whereas others are focused on the characteristics of the offenders and their methods. In determining the impact of the offence, some countries look at the financial losses as a proportion of the victim's annual income, or the amount of money stolen, whether computer devices have been used or whether a recidivist or organized criminal group is involved (see examples below).

### LEGISLATIVE EXAMPLE: MEXICO



#### FEDERAL CRIMINAL CODE

Article 386. Any person who acquires something illicitly or achieves an undue gain by deceiving another person or taking advantage of that person's error shall be guilty of the offence of fraud.

The offence of fraud shall be punishable by the following penalties:

- I. Imprisonment for a term of three days to six months or a fine of 30 to 180 day-fine units if the value of the property acquired through the act of fraud is not more than 10 times the minimum wage;
- II. Imprisonment for a term of six months to three years and a fine of 10 to 100 times the minimum wage if the value of the property acquired through the act of fraud is more than 10 times but not more than 500 times the minimum wage;
- III. Imprisonment for a term of 3 to 12 years and a fine of up to 120 times the minimum wage if the value of the property acquired through the act of fraud is more than 500 times the minimum wage.

<sup>&</sup>lt;sup>299</sup>These factors are compiled to summarize the legal frameworks of the different countries. Not all factors were present in the legislative frameworks for each country. Examples of aggravating factors include: victim experience (large financial or other personal impact (e.g. instilling fear or a sense of danger in the victim)); large financial loss to individuals or across victims; large scale in terms of the volume of victims and/or amount of money lost; targeting victims who are in some way vulnerable; targeting the State, public institutions or charity; fraudster characteristics (involvement of an organized criminal group or gang; recidivist offenders); and categories of fraud (computer or electronic fraud; involving the issuing of shares, bonds, warrants or securities; involving impersonation of a public official, abuse of an official position or abuse of personal relations).

## LEGISLATIVE EXAMPLE: UZBEKISTAN



### CRIMINAL CODE

Article 168. Fraud

Fraud, that is, acquisition of someone's property or the right thereto by deception or abuse of confidence,

shall be punished with a fine up to 100 times the minimum monthly wage, or correctional labour for up to one year or imprisonment for up to six months.

### Fraud committed:

- (a) On a large scale;
- (b) Repeatedly or by a dangerous recidivist;
- (c) By previous concert by a group of individuals;
- (d) With the aid of computer devices;

shall be punished with a fine from 100 to 300 times the minimum monthly wage, or correctional labour for up to two years or imprisonment for up to five years.

### Fraud committed:

- (a) On a large scale;
- (b) By a special dangerous recidivist;
- (c) By an organized group or in its interests;

shall be punished with a fine from 300 to 600 times the minimum monthly wage, or correctional labour for up to three years or imprisonment from 5 to 10 years.

In the instance of compensation for the pecuniary damage, the penalty of imprisonment shall not be applied.

The sentence bands are also highly variable. In some countries (e.g. Uruguay), four years' imprisonment is the maximum sentence, whereas in other countries (e.g. United States) there is provision for sentences as high as 30 years' imprisonment. In some other countries, there are no stipulated sentence bands, with sentences likely dependent on prosecutorial discretion or the application of a general criteria for determining the seriousness of crime.

### LEGISLATIVE EXAMPLE: UNITED STATES OF AMERICA



### TITLE 18

Article 1344. Bank fraud

Whoever knowingly executes, or attempts to execute, a scheme or artifice:

- (a) To defraud a financial institution; or
- (b) To obtain any of the moneys, funds, credits, assets, securities, or other property owned by, or under the custody or control of, a financial institution, by means of false or fraudulent pretences, representations, or promises;

shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

## Law enforcement

Law enforcement has an important role to play as part of a wider strategy that is focused on preventing fraud and protecting the public. Criminal justice can act as a deterrent to discourage offenders or would-be offenders, provides for punishment, protects society from harmful offenders and reinforces social values on accepted behaviours.<sup>300</sup> The capacity to deliver robust law enforcement is affected by the factors set out below.

## Assessing and targeting organized fraud

In the context of the varied and competing demands of organized crime, policing resources commonly gravitate to crimes other than fraud.<sup>301</sup> In tackling organized fraud, criminal sentences can be insufficient, information can be lacking and, perhaps more fundamentally, uncertainties can exist on how to integrate fraud into policies against serious and organized crime. The inability to identify these intersections can leave organized fraudsters untouched by law enforcement. Clear and robust policy and legislative frameworks help to more clearly identify fraud cases that constitute serious and organized criminal cases and strengthen assessments in law enforcement for targeting proactive criminal investigation resources.

## Criminal investigation

There are concerns in many regions that the police may not be prepared or equipped to address the growth in cyberfraud. This relates partly to law enforcement policies, systems and culture that have struggled to adapt to this new criminal landscape. <sup>302</sup> Some law enforcement agencies have established specialist units with capabilities in fraud and cybercrime investigation, commonly focused on undertaking the most complex investigations to target the highest-risk offenders. <sup>303</sup> Key resources include a capability to engage in effective digital investigation, practitioners with expertise in financial investigation and digital forensics, and technology to facilitate investigative procedures.

## Disruption

Organized fraud can be perpetrated in high volumes and at a speed that is often at odds with the slow pace of complex fraud investigations. Disruption can draw from a wide range of techniques and capabilities available to law enforcement and partner organizations, to offer more diverse tactics to impede the capacity of criminals to offend and thus to reduce the risk of further harm to the public. Tactics can be targeted at the acts, actors or criminogenic environments, with key examples including website takedowns; the seizure of criminal proceeds; the targeting of key individuals in a network such as those facilitating money-laundering or supplying stolen personal information; and interventions to disrupt co-offending, such as tactics to undermine trust in criminal marketplaces.

<sup>300</sup> Button and others, Fraud and Punishment.

<sup>301</sup> Doig and Levi, "A case of arrested development?".

<sup>&</sup>lt;sup>302</sup> Adam M. Bossler and Tom J. Holt, "Patrol officers' perceived role in responding to cybercrime", *Policing: An International Journal of Police Strategies and Management*, vol. 35, No. 1 (March 2012); and Barry Loveday, "Still plodding along? The police response to the changing profile of crime in England and Wales", *International Journal of Police Science and Management*, vol. 19, No. 2 (April 2017).

<sup>&</sup>lt;sup>303</sup> Mark Button and Martin J. Tunley, "Explaining fraud deviancy attenuation in the United Kingdom", *Crime Law and Social Change*, vol. 63, Nos. 1 and 2 (March 2015); and Dale Willits and Jeffrey Nowacki, "The use of specialized cybercrime policing units: an organizational analysis", *Criminal Justice Studies*, vol. 29, No. 2 (April 2016).

<sup>&</sup>lt;sup>304</sup> Michael Skidmore, "Lifting the lid on 'disruption' as an approach to controlling serious and organised crime", Perspectives on Policing Paper, No. 9 (London, The Police Foundation, 2023).

<sup>&</sup>lt;sup>305</sup>To illustrate, law enforcement agencies from multiple countries targeted a criminal website that supplied software for criminals to make automated calls that spoofed legitimate services. This disrupted the supply of software that was estimated to have been used to make 10 million fraudulent calls to members of the public and caused losses of €115 million (Europol, "Online fraud schemes"). See also Alice Hutchings and Thomas Holt, "The online stolen data market: disruption and intervention approaches", *Global Crime*, vol. 18, No. 1 (2016).

## International cooperation

It is common for the offenders, victims, technologies and other enablers of organized fraud to be transnational, which can cause confusion over jurisdiction and hamper localized criminal investigations. This is due, inter alia, to the challenges in quickly leveraging mutual legal assistance from other countries, particularly for acquiring and sharing data and evidence from the private sector to facilitate investigation and prosecution, as well as complex extradition processes.<sup>306</sup> International cooperation is also important for seizing and confiscating criminal proceeds, returning stolen assets and ensuring compensation for the victims.<sup>307</sup>

### Diverse workforce

People have different experiences with the criminal justice system, due to factors such as racism, sexism, ableism, homophobia and discrimination on the grounds of socioeconomic status. The ability for these experiences to be adequately addressed is limited due to the continued underrepresentation of women and persons from diverse backgrounds in law enforcement entities, the criminal justice system and decision-making positions, with research<sup>308</sup> finding that female officers are better positioned to meet the needs of women and girls in their communities. Despite this, UNODC has found that the percentage of women police officers across all the countries studied varied between 3 and 37 per cent.<sup>309</sup>

### CASE STUDY: REGIONAL AGREEMENT FOR TACKLING ORGANIZED FRAUD



China and the Association of Southeast Asian Nations, in conjunction with the United Nations Office on Drugs and Crime, have developed a transnational strategy to improve national, bilateral and regional responses to trafficking in persons and casino and scam operations. A key aim is to increase the capacity of law enforcement agencies and criminal justice practitioners to respond in a comprehensive and coordinated way. A regional focal point network was established to assist in the sharing of information and the coordination of criminal investigations and to facilitate the provision of timely responses to requests for assistance from nations in the region. Furthermore, the network serves to build capacity across members in cybercrime investigations, digital forensics, the handling of digital evidence, virtual assets and financial investigations. It also undertakes work to review and strengthen the implementation of legislative and policy frameworks to address crimes linked to casino and scam operations and enhance cooperation with the private sector, regional bodies and civil society.

Source: UNODC, Regional Office for South-East Asia and the Pacific, "ASEAN member States and the People's Republic of China regional cooperation roadmap to address transnational organized crime and trafficking in persons associated with casinos and scam operations in South-East Asia" (Bangkok, 2023).

<sup>&</sup>lt;sup>306</sup> Eva Nagyfejeo, "EU's emerging strategic cyber culture(s)", Policing: A Journal of Policy and Practice, vol. 15, No. 1 (March 2021).

<sup>&</sup>lt;sup>307</sup> For example, the Joint Cybercrime Action Taskforce in Europol coordinates operational activity to target transnational payment fraud, and Eurojust facilitates the provision of legal assistance and cooperation between member countries (Eurojust, "Actions across Europe against online fraud with cryptocurrencies", press release, 7 November 2023). See also South-East Asia Justice Network, available at <a href="https://www.unodc.org/roseap/en/SEAJust/index.html">www.unodc.org/roseap/en/SEAJust/index.html</a>.

<sup>&</sup>lt;sup>308</sup> UNODC, INTERPOL and United Nations Entity for Gender Equality and the Empowerment of Women (UN-Women), Women in Law Enforcement in the ASEAN Region (Bangkok, 2020).

<sup>&</sup>lt;sup>309</sup> UNODC, Issue Paper: Organized Crime and Gender.

# Intelligence-led policing

Organized fraud typically crosses jurisdictional borders by enlisting co-offenders who are geographically dispersed, targeting victims across multiple jurisdictions and using technology providers that are overseas. Organized fraud that is geographically dispersed may not align with the priorities of territorial policing, which are focused on a localized rather than a cross-border agenda and which are bound to discrete and localized jurisdictions, data and systems. Visibility is contingent on taking a national or international perspective to offending. Furthermore, not all fraud is felt acutely by each individual victim: the impact is diffuse, and it is only when viewed in the aggregate that this offending becomes serious, for example, by virtue of the fraudsters perpetrating high volumes of fraud, acquiring large criminal profits or undermining the trust and integrity of legitimate systems.<sup>310</sup> The ability to assess harm in this context is contingent on the availability of information to connect offences and identify persistent offending and associated risks.

Identifying organized fraud relies on compiling data sets and analysing connections between data points to draw out intelligence on organized criminal groups. A single victim reporting a fraud may have limited knowledge of the offenders and their methods; patterns in offending and the corresponding risks of organized crime are identified through processes of data analysis to connect separate offences and produce the intelligence required for a proactive policing response. A model of policing that is singularly focused on delivering reactive criminal investigations of reported crimes commonly fails to reach below the surface and address the underlying fraudulent scheme, because organized fraud is seldom revealed in an isolated fraud report.

# Protection of persons affected by organized crime

Fraudsters employ techniques of social engineering to exploit the human psychological and behavioural factors that make people vulnerable to deception and manipulation.<sup>311</sup> Consequently, effective crime prevention is contingent not only on developing more secure systems, but also on equipping the public and business community with the knowledge, awareness and capabilities to defend against fraud. Fraud is highly diverse and continuously evolving, and the effectiveness of education and awareness-raising campaigns lies in public messaging that is succinct and clear enough to influence public behaviours and vigilance.<sup>312</sup> The effectiveness also lies in the accessibility of such campaigns, including the consideration of the different languages spoken by specific population groups and accessibility measures for persons with disabilities. Vulnerability is often context-specific and public information may need to be designed with and targeted at people who are engaging in specific markets or activities where there are risks.<sup>313</sup> Furthermore, vulnerability is not static: it oscillates according to the victim's circumstances and the specific methods that are employed by the fraudsters. Therefore, there can be a need for prevention messaging to reach an at-risk individual or business at the right time.<sup>314</sup>

<sup>&</sup>lt;sup>310</sup>Levi, "Organized fraud and organizing frauds".

<sup>&</sup>lt;sup>311</sup> Brandon Atkins and Wilson Huang, "A study of social engineering in online frauds", *Open Journal of Social Sciences*, vol. 1, No. 3 (August 2013).

<sup>&</sup>lt;sup>312</sup>See, for example, European Commission, Anti-Fraud Knowledge Centre, Library, Good practices, "#Fraudoff", available from the European Union Funds Anti-Fraud Knowledge and Resource Centre (<a href="https://antifraud-knowledge-centre.ec.europa.eu/">https://antifraud-knowledge-centre.ec.europa.eu/</a>); and Cassandra Cross and Michael Kelly, "The problem of 'white noise': examining current prevention approaches to online fraud", *Journal of Financial Crime*, vol. 23, No. 4 (October 2016).

<sup>&</sup>lt;sup>313</sup> For example, the Securities and Exchange Commission in the United States delivers targeted education to prospective investors to improve their knowledge of the market and help them to defend against fraud (see https://www.investor.gov/about-us).

<sup>&</sup>lt;sup>314</sup>The Cyber Security Information Sharing Partnership in the United Kingdom is aimed at helping businesses securely share real-time information on dynamic cyberthreats, thereby ensuring that member organizations are aware of the emergent risks and can implement countermeasures (United Kingdom, "Government launches information sharing partnership on cyber security", press release, 27 March 2013).

Fraudsters can target the same individual on multiple occasions, such as in some cases of romance and investment fraud, by means of grooming or manipulation by the perpetrator or on the basis of a personal vulnerability;<sup>315</sup> these victims may not recognize that they are being defrauded and may not report the fraud to the police. Financial and other intelligence sources can help identify at-risk victims and drive proactive safeguarding responses from law enforcement entities and other organizations in the public and private sectors.<sup>316</sup>

# Promotion of partnerships and cooperation

### National data collection

Information on fraud comes from a range of sources and in various forms. It includes reports on crime and intelligence received from members of the public, private corporations and small businesses that have been targeted or defrauded, reports and intelligence collected by public sector regulators or the private sector and reports collected by consumer advocacy organizations or other sources. Law enforcement agencies do not have a monopoly on fraud data, and these varying sources mean that it is difficult to compile a comprehensive crime picture to demonstrate the scale and nature of the problem. The fragmentation of the data means that there are challenges for State agencies in identifying and tracking key patterns and trends, assessing risks, assigning roles and resources and developing robust strategies. There is also a lack of gender-disaggregated data on the issue, which affects the ability of national authorities to understand gender trends and the intersecting characteristics that shape people's experiences with organized fraud. However, there are a number of measures that can be taken to produce a more consolidated picture. These measures are described below.

## Centralized fraud reporting

The fragmented reporting landscape can have an impact on victims and their experiences of seeking the help and support they need. They can be faced with a bewildering landscape of public and private sector entities and civil society organizations offering a wide range of support, and finding the right service can involve a prolonged process of trial and error, with victims passed from one organization to the next.<sup>318</sup> This problem can be exacerbated by weak responses from the police, especially in regionalized teams that have limited capability to engage in complex and cross-border investigations. The provision of reporting channels that are streamlined and connected helps to ensure that victims receive the support they need, while also consolidating the national picture on fraud and victims thereof.

<sup>&</sup>lt;sup>315</sup> See, for example, Elisabeth Carter, "Confirm not command: examining fraudsters' use of language to compel victim compliance in their own exploitation", *The British Journal of Criminology*, vol. 63, No. 6 (November 2023).

<sup>&</sup>lt;sup>316</sup>One example from Australia involved the police, in partnership with the government department for commerce, monitoring international money transfers to high-risk countries to identify and engage individuals suspected of being victims of fraud (Cross and Blackshaw, "Improving the police response to online fraud").

 $<sup>^{317}</sup>$ Levi and Burrows, "Measuring the impact of fraud in the UK".

<sup>318</sup> Button and others, "Not a victimless crime".

### CASE STUDY: CENTRALIZED REPORTING



In Australia, the National Anti-Scam Centre is one example of a government-led initiative to make it easier for victims to report fraud. The centre has a consumer protection focus and adopts the principle of "no wrong door" whereby, regardless of individual circumstances and needs, all fraud victims are provided with support. In other countries there has been a focus on consolidating crime recording systems by introducing national reporting centres for victims of fraud and cybercrime. For example, in the United States of America, the Internet Crime Complaint Center, operated by the Federal Bureau of Investigation, receives all public reports of Internet crime, including fraud.

Sources: Australia, National Anti-Scam Centre, "National Anti-Scam Centre in action", Quarterly update (July-September 2023); and www.fbi.gov/video-repository/ic3\_112117.mp4/view.

The availability of a single responsible and authoritative body for receiving crime reports eases the process of reporting for victims, which is particularly important in fraud when considering the high levels of underreporting.<sup>319</sup>

## Integrating data sets

In order to combat fraud, strategic partnerships with the private sector and other stakeholders are indispensable, including for the purpose of the development of legal frameworks for sharing crime data and intelligence. A high volume of fraud targets institutions such as banks, other financial service providers, e-commerce and other companies. This is often done by means of legitimate customer accounts (e.g. account takeover or consumer fraud), and many individual victims report such fraud to their service provider instead of the police. Furthermore, private sector companies engage in complex data analytics to identify risks and defend against fraud or can even initiate their own internal investigations to identify perpetrators. Channels are needed to ensure that these data can be easily shared with law enforcement or other public bodies.<sup>320</sup>

Integrating data sets from different sectors helps compile a more complete strategic picture of the problem. This shared information can also be used to leverage tactical responses to crime and crime-related risks that may otherwise remain hidden. Such responses include intelligence-led law enforcement activity and harm reduction interventions to flag risks and protect individuals or businesses from becoming victims of fraud.

## Public-private sector partnerships

Organized fraud seldom takes place in the public spaces that are within the control of the State, but rather in spaces that are under the commercial control of private sector intermediaries that provide Internet-based communications, e-commerce, financial services, web applications and telecommunications. Private sector businesses design the technologies and systems that perpetrators incorporate and exploit as part of fraudulent schemes. They are also central to the landscape as victims, providers of online security, sources of information to understand this offending, and hubs of counter-fraud expertise and capability. They have a particularly important role in designing and implementing strategies that remove the vulnerabilities in systems that are exploited by criminals, with a view to mitigating future

<sup>&</sup>lt;sup>319</sup> For instance, only 17 per cent of fraud experienced by the public in the United Kingdom in the 12-month period April 2016–March 2017 was reported to the police (United Kingdom, Home Office, *The Scale and Nature of Fraud: A Review of the Evidence* (2018)).

<sup>&</sup>lt;sup>320</sup> In the United Kingdom, the police have developed a close partnership with Cifas and United Kingdom Finance, which collect data on fraud that targets their membership organizations, which include key stakeholders in financial services. See, for example, United Kingdom, Office for National Statistics, "Crime in England and Wales: year ending June 2023", 19 October 2023.

risks of organized fraud. The scope for tackling organized fraud is contingent on fostering cooperation with private sector businesses that individually and collectively govern the digital domains that provide a fertile ground for fraud.

The capacity for private sector intermediaries to take action against organized fraudsters will vary according to their functions and how direct their business relationship is to the person using their services for a criminal purpose. Under the strategic principles of promoting cooperation and partnerships in a whole-of-society approach to tackling organized crime, private sector intermediaries can adopt a range of key roles,<sup>321</sup> such as:

- Identifying suspected criminal actors and activity and notifying the authorities or intended victims accordingly (including whistle-blowing with regard to internal fraud)
- Preventing fraudulent communications from reaching victims such as by removing or blocking malicious websites, advertisements or profiles
- Providing gender-disaggregated data to augment the strategic intelligence picture and facilitate criminal investigations
- Preventing the loss of funds that are transferred to offenders
- Educating their service users about fraud and raising awareness of it in an accessible manner tailored to different target groups
- Designing systems and policies that minimize and alleviate the risk of fraud

In cases where fraud presents a threat to a business or sector, strategies may be guided by internalized needs and objectives.<sup>322</sup> In some cases, the systems in different sectors or businesses can act as a conduit for fraud that has an impact on external actors or bodies, such as members of the public or other sectors. For example, the use of telecommunications to send fraudulent text messages is a type of fraud experienced by individual victims and financial service providers that process the payments or transfer requests.

Taking a strategic perspective across a range of sectors makes it easier to identify system-wide vulner-abilities in technological, commercial or financial infrastructure. One approach is to strategically account for the key stages in perpetrating certain types of fraud and identifying the convergences with technologies, products and services, including, for example, the inbound channel for making initial contact with victims (e.g. social media advertisements), the interaction with victims (e.g. spoofed messages) and the processes of cashing out to access the criminal proceeds (e.g. payment systems).

Coordination needs to be done in a way that considers the range of industries and organizations that make up this infrastructure, including global corporations and smaller businesses, businesses located within the country and those that operate outside of the legal jurisdiction, and businesses with access to various resources and capabilities for assisting in counter-fraud work.<sup>323</sup> There are various means of incorporating the private sector into a coordinated approach, which include fostering strategic partnerships between the State and the private sector and civil society organizations,<sup>324</sup> establishing and agreeing on standards or voluntary principles to help steer more consistent policies and practices

<sup>&</sup>lt;sup>321</sup> UNODC, "Organized crime strategy toolkit".

<sup>&</sup>lt;sup>322</sup> For example, the Southern African Fraud Prevention Service facilitates the sharing of information among member companies to identify and address internal risks of fraud (see <a href="www.safps.org.za/Home/About">www.safps.org.za/Home/About</a>).

<sup>&</sup>lt;sup>323</sup>See, for example, Michael Levi and Matthew Leighton Williams, "Multi-agency partnerships in cybercrime reduction: mapping the UK information assurance network cooperation space", *Information Management and Computer Security*, vol. 21, No. 5 (November 2013).

<sup>324</sup> See, for example, United Kingdom, Home Office "Joint fraud taskforce", 17 October 2017.

across businesses, and establishing statutory regulations to impose duties on key stakeholders in the private sector.<sup>325</sup>

It is important to break down the key stages of fraud to help identify the strategic pinch points for targeting crime prevention activity. There are multiple examples in which public-private partnerships have been cultivated to implement strategies for preventing systemic vulnerability. The case studies set out below represent initiatives for tackling each of the stages of fraud outlined above.

### CASE STUDY: CROSS-SECTOR RESPONSE TO MALICIOUS WEBSITES



The National Cyber Security Centre in the United Kingdom of Great Britain and Northern Ireland has agreements with Internet service providers in the United Kingdom to share real-time information on websites that have been identified as fraudulent. The providers are then able to block access to the fraudulent websites and prevent the associated fraudsters from communicating with prospective victims in the United Kingdom.

Source: United Kingdom, National Cyber Security Centre, "NCSC joins industry to offer unprecedented protection for public from scams", 11 May 2022.

# CASE STUDY: CROSS-SECTOR RESPONSE TO MASS COMMUNICATION BY TEXT MESSAGE



In a bid to stem the high volume of smishing that exploits telecommunications to impersonate legitimate organizations, the Australian Communications and Media Authority has introduced a text message sender registry. The system encourages the participation of key industry stakeholders to establish a directory of trusted senders in order to restrict the capacity for criminals to send bulk text messages that impersonate (or spoof) these organizations. This would serve to filter out malicious messages purporting to represent these organizations and thus prevent them from reaching prospective victims.

Source: Parliament of Australia, "Telecommunications Amendment (SMS Sender ID Register) Bill 2024", available at <a href="https://www.aph.gov.au/">www.aph.gov.au/</a>.

<sup>&</sup>lt;sup>325</sup> For example, the European Union Digital Services Act will introduce new obligations for online marketplaces to trace vendors on their platform to help pursue fraudsters more effectively. See <a href="https://ec.europa.eu/commission/presscorner/detail/en/qanda\_20\_2348">https://ec.europa.eu/commission/presscorner/detail/en/qanda\_20\_2348</a>.

# CASE STUDY: CROSS-SECTOR HUB FOR PREVENTING THE LOSS OF MONEY TO FRAUD



In Singapore, the Anti-Scam Command is a centralized police unit that has forged close partnerships with a range of financial service providers, some of which are co-located with the police unit. Stakeholders include local and foreign banks, card security groups, fintech companies and cryptocurrency houses. This integrated approach enables quick-time information-sharing and analysis of financial intelligence to identify and block financial transfers that are suspected of being fraudulent. Online payments and wire transfers allow fraudsters to rapidly move and cash out stolen funds, and the aim of this collaboration is to swiftly freeze accounts, recover funds and thereby reduce losses to victims.

Source: Singapore Police Force, "Opening of anti-scam command office", 6 September 2022.

Effective responses to fraud also need to take into account the regulatory landscape for controlling the provision of products and services. The accessibility of these products and services provides the camouflage to conceal fraudulent schemes and deceive victims. Regulation has a key role in implementing effective trust mechanisms to prevent malicious actors operating from within legitimate sectors. This includes public and private sector regulators adopting robust "know-your-customer" principles when opening bank accounts, applying for the use of other enabling services such as payment services, telecommunications and other business services (e.g. office rentals) and registering companies or professionals (e.g. financial service practitioners).

The crimes encompassed by organized fraud traverse national borders, industries and demographic groups. This creates complexities in developing policies and delivering responses that are effective. There are key foundational steps that each State can take, firstly to understand how organized fraud manifests and has an impact within its borders and secondly to design and deliver effective strategic responses across the four pillars for tackling organized crime (prevent, pursue, protect and promote). Policymaking must also account for the transnational context of organized fraud in order to ensure the delivery of coordinated international responses. Moreover, organized fraud calls for a whole-of-society response that incorporates strategic partnerships with key non-government stakeholders, particularly in the private sector, to produce a more enhanced understanding of the problem and craft strategies against it.

# Conclusion

Organized fraud represents a multifaceted and pervasive threat that transcends borders, industries and demographics. Addressing this complex issue necessitates a comprehensive approach, beginning with the development of a common language and understanding of the different categories of organized fraud.

The present issue paper is aimed at contributing to the scholarship by providing an overview of organized fraud that targets individual members of the public or private institutions for the purposes of obtaining a financial or other material benefit. The fraud categories developed here take a victim-centred perspective and therefore have a primary focus on the narrative or ruse that is presented to the victims. While comprehensive, the issue paper is not exhaustive, and there remains a myriad of possible issues relevant to organized fraud. More research from scholars, practitioners and civil society is needed to develop our knowledge and understanding of a highly diverse and complex area of crime.

The organized fraud categories presented in the issue paper are intended to provide stakeholders with a better understanding of the issue, with a view to fostering effective multi-stakeholder strategies to prevent organized fraud, pursue organized criminal groups, protect persons affected by organized fraud and promote partnerships and cooperation, as well as safeguarding victims and enhancing societal resilience against this persistent threat. Collaboration across sectors, continuous innovation and unwavering commitment to upholding justice and human rights are essential for mitigating the impact of organized fraud and promoting a safer and more secure global environment.

Nevertheless, much remains to be done. The issue paper on organized fraud is one part of a broader project that will develop additional tools and research to prevent and combat organized fraud, including measures to strengthen legislation, raise public awareness and defences and foster effective cooperation with private and other sectors, to name a few. By continuing to advance understanding and response capabilities, significant strides can be made in protecting individuals and institutions from the pervasive threat of organized fraud.







Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria Tel.: (+43-1) 26060-0, Fax: (+43-1) 263-3389, www.unodc.org

