In AI we trust – The use of artificial intelligence tools for payment fraud detection

Grazia Bruzzese

Abstract: Notwithstanding the various denominations it gained throughout time and its various subsets, it can reasonably be argued that fraud is a phenomenon present since the beginning of History. From the Roman Laws of the Twelve Tables which already covered the action of *fraus*, to its more modern and famous forms, like Ponzi schemes, fraud is recognized and sanctioned by the various legal systems throughout the globe. Yet, despite it being well-known since the Antiquity, the different forms that fraud can take are definitively not set in stone.

New technologies, like Artificial Intelligence, have not only touched upon all the sectors but also changed the traditional ways we deal with daily businesses. More specifically in the context of fraud, the development of a new subset of varieties like digital payment frauds can be witnessed. Nonetheless, new challenges go often hand in hand with new opportunities. As a result, if the use of new technologies has certainly inspired criminal minds to develop new illicit actions, it also opened the doors to new ways of detecting and contrasting them.

This contribution is intended to provide a short study of a specific type of digital financial fraud, namely digital payment fraud, by presenting some of the existing Artificial Intelligence tools that are currently used for the purpose of its detection. By relying on publicly available data, it will present and evaluate some of the strengths and weaknesses of these tools all while reflecting upon further avenues for improvement in the use of such technologies

Introduction. From bottomry to phishing: 2500 years of fraud – 1. Defining fraud in the digital age era: Setting the scene for AI-based countermeasures – 2. A spectre is haunting banking services: digital payment fraud – 2.1. Defining the subject – 2.2. On the various shades of digital payment fraud – 3. Beyond human eyes: AI's fight against digital payment fraud – 3.1. Every rose has its thorn: The Double-Edged Sword of Machine Learning in Fraud Detection – 3.2. Sharing is caring? – Conclusion

Introduction – From bottomry to phishing: 2500 years of fraud

"No sooner has the name OEDIPUS passed his lips, than his voice is drowned in a shout of execration. They call upon him to leave Attica

instantly. He won their promise by a fraud, and it is void"[1], wrote Sir Richard C. Jebb in his commentary of *Oedipus at Colonus*. This remarkable comment of the Sophoclean tragedy witnesses the opprobrium that the inhabitants of Colonus showed toward Oedipus, initially defrauding them by hiding his identity. In addition to reflecting a sentiment that has persisted for over two millennia in response to fraudulent behaviour, this passage highlights the enduring nature of fraud as a social phenomenon that continues to pose significant challenges in contemporary societies. Undoubtedly, fraud constitutes a legally complex and polymorphic phenomenon, characterized by its protean nature and resistance to precise categorization within a singular doctrinal framework. Although it has existed throughout history—arguably intrinsic to human conduct—fraud distinguishes itself from other offences by its capacity to evolve in form and function across different legal systems and historical periods. Unlike many other criminal offences, it continually adapts to the socio-economic and cultural contexts in which it occurs.[2] As such, it must be understood not only as a breach of legal norms but also as a socio-legal construct that reflects the prevailing values and normative expectations of the society and the era in which it occurs.

Fraud has been present since antiquity, if not before, with one of the earliest documented cases dating back to approximately 300 B.C. This recorded case involved a Greek merchant, by the name of Hegestratos, who attempted to perpetrate an insurance fraud through a maritime loan arrangement known as *bottomry*.[3] Under this mechanism, the merchant

1 Richard C Jebb, "Parodos: 117–253", in *Commentary on Sophocles: Oedipus at Colonus,* 1899.

2 Cf. for an overview on the evolution of fraud: Aurora AC Teixeira, António Maia, José António Moreira, Carlos Pimenta (eds), *Interdisciplinary Insights on Fraud* (Cambridge Scholars Publishing 2014); Martin T Biegelman, *Faces of Fraud: Cases and Lessons from a Life of Fighting Fraudsters* (Wiley 2013). Sridhar Ramamoorti, David E Morrison III, Joseph W Koletar, Kelly R Pope, *A. B. C. 's of Behavioral Forensics: Applying Psychology to Financial Fraud Prevention and Detection* (Wiley 2013). Elisabeth B Haarington, 'The Sociology of Financial Fraud', in Karin K Cetina, Alex Preda (eds), *The Oxford Handbook of The Sociology of Finance* (Oxford University Press 2012), 393–410. J.T. Wells, *International Fraud Handbook* (Wiley 2018).

3 Cf. Christian Chavagneux, *Les plus belles histoires de l'escroquerie* (Éditions du Seuil 2020) 1–17. Interestingly enough, bottomry seems to have persisted with regard to maritime business to the point where some cases were to be found in the XVIIIth century. Cf. Maria Fusaro, Andrea Addobbati, Luisa Piccinno (eds.), *General Average and Risk Management in Medieval and Early Modern Maritime Business* (Palgrave Macmillan 2023).

secured a loan by insuring a shipment of a given good. Yet, instead of fulfilling the terms of the agreement by delivering the good, he would set sail without the insured cargo (his plan further involved selling the corn elsewhere for additional gain), intending to deliberately scuttle the vessel and thereby retain the loan proceeds. Indeed, the insurance consisted in the fact that if the ship sank, the loan did not need to be paid back.[4] Fraud's capacity to permeate all levels of society is evident across history. As a matter of fact, it is capable of reaching and affecting even the most illustrious and powerful people in a given society as illustrated in the very famous 'affair of the Diamond Necklace' which involved and tarnished the reputations of Cardinal de Rohan and Queen Marie Antoinette.[5] Affecting the private finances of poor small investors – like it is often the case when it comes to Ponzi schemes – or even public funds, it is sufficient to think of fake president frauds against public institutions or non-governmental organisations partially or entirely funded by governments, like the recent fraud scandal against Caritas Luxembourg.[6]

Yet, despite the apparent heterogeneity of these cases – ranging from insurance fraud to political scandals and complex financial schemes – they are all subsumed under the legal category of fraud. This convergence of disparate cases under the umbrella term of fraud not only suggests the adaptability and definitional boundaries of fraud but also invites reflection on the elasticity and new configurations of fraud as a legal construct within contemporary legal systems. To this end, this book chapter will proceed in three parts. The first part offers a conceptual overview of fraud, tracing its historical evolution all while providing the necessary foundation for understanding how technological changes have reshaped it. The discussion subsequently turns to the financial sector, examining the phenomenon of digital payment fraud. The role of Artificial Intelligence (hereafter 'AI') in combating these practices will be assessed, focusing on both its potential and its inherent risks. The chapter concludes by drawing together these elements to reflect on the broader implications of AI fraud detection systems for the stability and integrity of financial systems.

4 Cf. Matthew Campbell, Kit Chellel, *Dead in the Water. Murder and Fraud in the World's Most Secretive Industry* (Atlantic Books 2022).

5 Cf. for more details on this affair: Chavagneux (n 3) 21 – 92.

6 On the Caritas case cf.: Véronique Poujol, 'Anatomie d'une affaire stupéfiante', in *Reporter.lu* (19 August 2024); Luc Caregari, 'Die globalen Folgen des Caritas-Skandals', in *Reporter.lu* (26 September 2024).

1. Defining fraud in the digital age era: Setting the scene for AI-based countermeasures

Given the breadth of its manifestations and typologies, the term *fraud* frequently functions as an umbrella concept encompassing a wide array of conducts that fall within the general ambit of fraudulent offences—ranging from payment fraud, romance scams, and Ponzi schemes to embezzlement, identity theft, and tax fraud, to cite just a few. Nonetheless, all these types of fraud, although committed through different operational mechanisms and with different means, share a set of common elements. Central among all these elements is the final goal namely, to obtain an advantage, in many cases, a pecuniary one – whether money or a valuable tangible good. In other words, it seems evident that fraud is intrinsically linked to money and financial gain. As a result, the latter is an offence pertaining to the realm of financial and economic criminal law. Apart from the expected material gain, fraud is characterised by the deployment of deceitful practices aimed at tricking and manipulating an individual into doing what the fraudster expects him or her to do, like proceeding to a payment or, in the context of phishing, clicking a malicious link that will compromise personal data. Hence, to say it in J. Scharfman's words, fraud is nothing else than a set of

> "multifarious means which human ingenuity can devise, and which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth. It includes all surprises, tricks, cunning or dissembling, and any unfair way which another is cheated. In its most basic form, a fraud can be thought of as a deception resulting in a loss. Fraud can occur anywhere and, in any amount, ranging from theft of a few dollars in the daily lives of consumers to complex corporate scams resulting in the loss of billions in cryptocurrency".[7]

To sum it up, and for the sake of clarity, fraud should be understood as a series of deceptive or misleading actions, carried out with the intent to procure a benefit or an advantage which the perpetrator would not otherwise be entitled to obtain.

To this already rich and complex framework, we must add a major historical and scientific revolution that has profoundly reshaped our societies, namely the development and proliferation of new technologies, frequently

7 Jason Scharfman, *The Cryptocurrency and Digital Asset Fraud Casebook* (Springer International Publishing AG 2023) 2.

referred to as the "Third Industrial Revolution".[8] It is undeniable that these new technologies, going from the rise of the internet to the phenomenon of AI, have altered the traditional modes of human activity, permeating all sectors of personal, professional and institutional life, to the point in which it is difficult to find one that remains unbothered. Given this pervasive impact, the fact that both legal and illegal activities would have been impacted should not come as a surprise. As a result, actors operating in the illegal world did not hesitate to take advantage of the new methods and schemes offered by new technologies. More specifically with regard to fraud, new technologies allowed for what some authors define "a new way to commit an old crime".[9] Indeed, as already proven, the offence of fraud is a polymorphous one, which did not hesitate to adapt and adopt new means like the internet or AI, giving rise to new forms of fraud that can be categorized under the umbrella term of "digital fraud" or "online fraud".[10] A new form of fraud that will be characterized by the fact that it is committed through the use of technological and digital means, whether simple fraudulent mails in the context of phishing, or the use of more sophisticated solutions relying on AI, like deepfakes.[11]

---

8 Giovanni Dosi, Louis Galambos, Alfonso Gambardella and Luigi Orsenigo (eds), *The Third Industrial Revolution in Global Business* (Cambridge University Press 2013); Manuel Castells, *The Information Age: Economy, Society and Culture* (Oxford: Blackwell 1996).

9 Susan W Brenner, 'Cybercrime Metrics: Old Wine, New Bottles?' (2004) 9 *Virginia Journal of Law & Technology* 13.

10 For a definition of "digital" or "online" fraud, cf. EUROPOL's Spotlight on Online Fraud Schemes: A Web of Deceit, according to which: *"Online fraud schemes (OFSs) comprise a wide range of criminal activities that are exclusively or primarily perpetrated online or with the use of computers; we call this cyber-enabled. […] Although online fraud specifically occurs online, such schemes can comprise both online and offline operations"*. In the context of our research, we will adopt the commonly acknowledged definition of digital fraud in the sense that we will refer to it whenever a fraud is committed in the online realm. See in *Europol Spotlight, Online Fraud Schemes: A Web of Deceit* (Europol 2023) 5, available at https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf (accessed on 2 March 2026).

11 To give a concrete example on the use of deepfakes in fraudulent schemes, reference may be made to a sophisticated fraud that took place in Hong Kong in 2024. In that case, one of the employees of a large multinational corporation was deceived into transferring funds exceeding $25 million. The deception was executed through a videoconference in which the employee believed he was interacting with colleagues and the company's chief financial officer; in reality, each of the participants had been digitally fabricated using deepfake technology. For more details on this case, cf. Kath-

From phishing to the use of deepfakes to deceive the victims all while hiding their identity, criminals did not fail to prove creativity in coming up with new means to commit fraud. Furthermore, not only did technology open the doors to new forms of fraud but, as pointed out by Interpol in its latest Global Financial Fraud assessment, it "is enabling organized crime groups to better target victims around the world".[12] A result that should not surprise considering the fact that we live in an increasing digitalised and interconnected world, in which, especially when it comes to finance, digital solutions are more and more taking over traditional means. It is sufficient to think about the way digital banking has revolutionised the way we interact with banks, from cashless and cardless payments, to the use of sophisticated financial robo-advisers,[13] a considerable number of traditional banking services can now be effectuated without any direct human interaction between the bank and the customer. The facilitation in defrauding victims using new technologies seems also to be the reason of the exponential worldwide rise in fraud cases.

To give some examples from the European Union (hereafter 'EU'), the last report by the European Anti-Fraud Office ('OLAF') has shown that over one billion euros (1.043.800.000 €) of EU funds were lost to irregularities, including fraud.[14] A sum that should be frightening if one considers the fact that OLAF's interests only revolve around the EU funds and not the ones of the various Member States. With regard to some of these Member States, the latest figures are not comforting either. In Italy for instance, 3.360 cases of internet fraud, more specifically investment scams, were reported only in 2023, amounting to 109.536.088 euros.[15] This same raise in

leen Magramo, 'British engineering giant Arup revealed as $25 million deepfake scam victim', *CNN* (17 May 2024) https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk accessed 24 July 2025.

12 Interpol, *Global Financial Fraud assessment* (May 2024), available at https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology accessed 13 March 2025.

13 Dan Tammas-Hastings, *Liability-Driven Investment: From Analogue to Digital, Pensions to Robo-Advice*,(Wiley 2021).

14 The European Anti-Fraud Office (OLAF), *OLAF Report 2023* (European Commission 2023). The report can be found at the following link: https://ec.europa.eu/olaf-report/2023/index_en.html. accessed 10 December 2024.

15 Ministero dell'Interno, *Resoconto attività 2023 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica* (2 January 2024) the report can be downloaded at the following link: https://www.interno.gov.it/it/notizie/report-2023-dellattivita-polizia-postale-nel-contrasto-crimini-informatici#:~:text=9.433%20quel-

fraud cases was witnessed in Luxembourg, where according to the police report for the year 2023, 6143 cases of fraud (*escroqueries/tromperies*) were reported, 1454 more than for the previous year.[16] France values the annual total amount of euros lost to fraud in 2023 to almost 1.2 billion euros.[17] Furthermore, according to the European Banking Authority ('EBA') and European Central Bank ('ECB') joint report, 2 billion euros only in the first half of 2023 were lost to payment fraud.[18] On the other side of the ocean the figures with regard to the money lost to fraud are not less impressive than the European ones. According to the latest data from the USA's Federal Trade Commission, the fraud losses reported in 2023 totalled more than $10 billion.[19]

Confronted with these exponential figures and having set the scene, it is now time to turn to a very specific type of fraud inherent to banking services, namely payment fraud, all while assessing how banks are trying to prevent and detect it through to the use of AI tools.

---

li%20commessi%20nel%202023,31%20casi%20di%20codice%20rosso. accessed 12 February 2025.

16 Police Lëtzebuerg, *Présentation des statistiques policières de la criminalité 2023*. The statistics can be downloaded at the following link: https://police.public.lu/fr/publications/2024/chiffres-de-la-delinquance.html. accessed 12 February 2025.

17 Banque de France, *Rapport de l'Observatoire de la sécurité des moyens de paiement 2023* (10 September 2024). The report can be found at the following link : https://www.banque-france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2023#:~:text=Rapport%20de%20l'Observatoire%20de%20la%20s%C3%A9curit%C3%A9%20des%20moyens%20de%20paiement%202023,-Mise%20en%20ligne&text=de%20dispositifs%20de%20blocage%20ou,%25%20par%20rapport%20%C3%A0%202022. accessed 30 March 2025.

18 European Banking Authority, *The EBA and ECB, 2024 Report on payment fraud* (1st August 2024) The report can be downloaded at the following link: https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud accessed 20 March 2025.

19 Federal Trade Commission, 'As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. Investment scams lead in reported losses at more than $4.6 billion' (9 February 2024) https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public accessed 30 March 2025.

2. A spectre is haunting banking services: digital payment fraud

We started this contribution by highlighting the multifaceted nature of fraud, including its continually evolving manifestations in the digital domain. Simultaneously, we stressed out one of the essential material elements of this offence, namely, the fact that the fraudster will illicitly try to gain a benefit, typically of a pecuniary nature. If one equates all these elements, it should not come as a surprise that one of the most prevalent and economically fruitful and consequential forms of fraud, as measured by financial losses incurred, is digital payment fraud.[20]

2.1. Defining the subject

As its designation already implies, *payment fraud* is a form of fraud perpetrated within the context of a *payment transaction*, as defined under the Payment Service Directive (hereafter 'PSD2').[21] According to the PSD2, a payment transaction refers to "an act, initiated by the payer or on his behalf or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee".[22] In other words, it is the simple fact for a payer to remit funds to a payee, *e.g.*, a customer paying a seller or service provider for a good or service s/he receives. Here again, while such transactions have existed since the beginning of time,[23] the advent of new technological infrastructures has transformed the means and modalities through which they are executed. Increasingly, these payment transfers are conducted via digital or cashless means, whether by

20 Cf. for some concrete data and figures: EBA and ECB, 2024 Report on payment fraud (1st August 2024). The report can be downloaded at the following link: https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud. accessed 30 March 2025.

21 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35.

22 Article 4(5) of the PSD2.

23 Cf. for a historical study of this subject: Jack Weatherford, *The History of Money* (Crown Currency 1998); Niall Ferguson, *Der Aufstieg des Geldes: Die harte Währung der Geschichte* (Econ 2009); Charles Eisenstein, *Sacred Economics: Money, Gift, and Society in the Age of Transition* (North Atlantic Books 2011); Viviana A Zelizer, *The Social Meaning of Money* (Basic Books 1995).

transferring credit through online payment orders or by simply using a credit card.

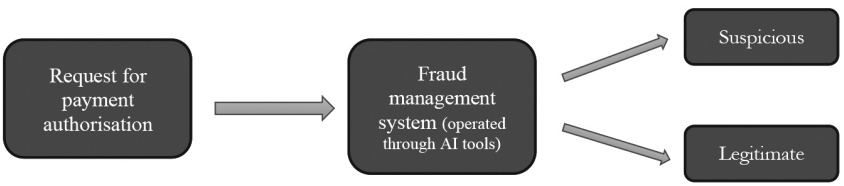
Although the execution of a digital or cashless payment appears to be a seamless and routine process, it nonetheless comprises a set of intricate and largely imperceptible procedural steps invisible to the eyes of the payer or of the payee. To give a simple illustration of how a cashless payment works, consider the common scenario in which a customer seeks to purchase a good, whether in a shop, by paying with a payment card, or online. To proceed with the payment, s/he will present the payment instrument, either the physical card or its digitalized version embedded within, for instance, its smartphone, and initiate the transaction by inserting it, or even more simple, just swiping it on a reader machine. A similar procedural framework can be transposed to the scenario where the transaction is executed via an online platform. In this scenario, the payer inserts the requisite payment credentials–typically pertaining to its card or bank account- into the designated fields on the digital interface, thereby initiating the transaction process.

This seemingly instantaneous act sets in motion a rather complex process made up of various steps. To present it in simple words, at the outset, a request for authorization to payment coming from the payee is transmitted to the payer's card issuer. The issuer will then analyze the request to assess whether the payment transaction shall be authorized or not. Once a decision authorizing or refusing the transaction has been made, it is then communicated and transmitted back to the payee.[24]

What happens in the process of deciding whether authorizing the transaction? This evaluative process involves multiple criteria. The card issuer will verify whether the payer truly disposes of the sufficient funds that s/he wants to spend, or in the context of credit instruments, whether the requested amount falls within the authorized credit limits. However, of relevance to the domain of payment fraud is the issuer's reliance on

24 Cf. for a more detailed presentation describing the engineering behind digital payments and its challenges: Nick F Ryman-Tubb, Paul Krause, Wolfgang Garn, 'How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark' (2018) 76 *Engineering Applications of Artificial Intelligence*, 130–157; Paolo Vanini et al., 'Online payment fraud: from anomaly detection to risk management' (2023) 9(1) *Financial Innovation*, 66–91; David S Evans and Richard Schmalensee, *Paying with Plastic: The Digital Revolution in Buying and Borrowing* (MIT Press 2004); Likhit Mada, 'The Rise of Mobile Payment Systems, Digital Wallets: Successes, Security and Challenges' (2025) 13(10) *European Journal of Computer Science and Information Technology* 137–152.

fraud detection and prevention mechanisms. Consequently, the decision on whether to authorize or not the transaction, will depend on the result of the so-called *fraud management system*. As the name already suggests, the aim of this control system is to verify that the transaction at hand is not an attempt to defraud the payer. To this end, the system is aimed at identifying anomalies in the transaction or indicators of potential fraudulent behavior, therefore safeguarding the transaction against unauthorized or deceitful activity.



Indeed, as shown by recent data,[25] out of the many risks to which financial and banking institutions are exposed to fraud remains one of the most pervasive and persistent ones. Consequently, an inquiry arises: in what manner does fraud manifest within this digital era context and affect the broader context of digital payments?

2.2. On the various shades of digital payment fraud

According to a recent study published by the Basel Committee on Banking Supervision[26], instances of digital payment fraud within the banking sector are usually categorised into four principal typologies. Considering the rise in online banking and online payment mechanisms, it should not come as a surprise that fraud related to unauthorized online payment transactions is

25 Cf. European Payments Council, *2024 Payment Threats and Fraud Trends Report* (22 November 2024) https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/202412/EPC16224%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf accessed 17 February 2025. EBA and ECB, *2024 Report on Payment Fraud* (1st August 2024) https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud accessed 10 February 2025.

26 Basel Committee on Banking Supervision, 'Discussion Paper Digital fraud and banking: supervisory and financial stability implications' (November 2023) https://www.bis.org/bcbs/publ/d558.htm accessed 30 March 2025.

one of the most common types of digital payment fraud. In this scenario, fraudsters unlawfully acquire customer data and, through its misappropriation, manage to access their online banking account or credit card credentials. A paradigmatic illustration of this form of fraud is the phenomenon of 'email phishing', in which fraudsters try, by emails, to make their victims give away sensitive information, for instance, credit card credentials, under the mistaken belief that the communication originates from a legitimate source, like their bank.

A second typology of digital payment fraud identified by the Basel Committee, is the one that arises when a payer is deceitfully manipulated into issuing a payment order under the false belief that the account belongs to a legitimate payee. In contrast to the first type of digital payment fraud, in this case the payer proceeds herself or himself to the payment order. In fact, this type of fraud is often perpetrated through the impersonation of a trusted third party, deceiving the payer into proceeding with the payment. As an example, one could think of the *CEO fraud* or *Fake President fraud*, in which the fraudster impersonates the CEO of a given company who gives instructions to one of the employees to proceed to a payment order which the employee will consider as legitimate.

Thirdly, digital payment fraud can also target bank customers by misleading them into investing in fictitious saving products, exploiting their trust in the bank. Such fraudulent schemes typically involve the presentation of false investment opportunities that appear to be legitimate banking products. We are referring to the notorious investment fraud or scams, in which fraudsters manage to induce victims to invest in non-existent investments. To this end, fraudsters will likely clone the website of legitimate firms, or simply promise the best possible returns, which are higher than the ones to be expected by investing in any other type of financial product, a technique which is at the very heart of Ponzi schemes and which nowadays seems to be more and more perpetrated through social media.[27]

Finally, digital payment fraud can also directly target banks themselves. In this case, fraudsters may provide the bank with false identities, or stolen ones, to open accounts or to proceed to payment orders. As a matter of

27 Akila Quinio, 'Advisers worry as social media investment scams urge', *Financial* Times (17 May 2024) https://www.ft.com/content/6f5055fc-08f6-4d83-9b66-414f7f09971e accessed 4 April 2025.

fact, there seem to be dedicated marketplaces on the dark web selling and purchasing payment card data and online banking access.[28]

Faced with challenges stemming from the use of new technologies not only by their customers, but, also, by fraudsters, financial and banking institutions could neither turn a blind eye on this phenomenon, nor rely upon obsolete and analogue-based safeguard solutions. Clearly, no one would nor could argue for a return to the complete previous analogue banking system, digital banking being nowadays too enshrined in our society. Similarly, there is no way to circumvent the use of new technologies which are going to increasingly dominate our daily activities and lives.[29] Hence, confronted with what may be characterized as an existential imperative to "adapt or cease to operate", the banking sector recognized the inadequacy of conventional fraud-detection methodologies[30] in addressing the evolving typologies of digital fraud.[31] Accordingly, the implementation of advanced

28 Cf. Basel Committee on Banking Supervision, Discussion Paper (n 26).

29 Cf. on this subject: Klaus Schwab, *The Fourth Industrial Revolution* (Clown Currency 2017); Felix Dodds et al., *Tomorrow's People and New Technology: Changing How We Live Our Lives* (Routledge 2022); Kevin Kelly, *The Inevitable: Understanding the 12 Technological Forces That Will Shape Our Future* (Viking 2016); Kai-Fu Lee and Chen Qiufan, *AI 2041: Ten Visions for Our Future* (WH Allen 2024).

30 For the sake of clarity, it is worth briefly specifying what we understand under the "old forms of fraud detection". Before the raise of AI tools especially those based on ML, the vast majority of fraud detection tools were run by a so-called "rule-based approach". Under this approach, it was necessary, as the name already suggests, to create in the sense of writing rules that would then be used to detect actions that deviated from these rules. To give a very banal example of the form that a written rule could take, one could decide that proceeding to a given number of transactions in a day should be seen as suspicious. Or, even more discriminatory, one could write a rule saying that payments directed to a given county should be flagged as suspicious and require further investigation. One of the main issues with the rule-based approach, despite the need for experts on the matter to write these rules, was the almost impossibility to rapidly adapt and keep up with the evolving types of fraud.

31 Recent data seem to prove the new trend toward the adoption of AI tools to prevent and fight fraud. Cf. for some national data on Luxembourg, Commission de Surveillance du Secteur Financier and Banque centrale du Luxembourg, (CSSF & BCL) *Thematic review on the use of Artificial Intelligence in the Luxembourg financial sector* (May 2025) https://www.cssf.lu/en/Document/thematic-review-on-the-use-of-artificial-intelligence-in-the-luxembourg-financial-sector-2/ accessed 2 March 2026. For a more global study on the use of AI tools to prevent and fight financial crimes, including fraud, cf. Napier AI, *AI/AML Index 2024–2025*, https://www.napier.ai/ai-aml-index accessed 2 March 2026. Cf. also for a study on the risks that come with an overuse of AI tools for crime prevention, Serhiy Lyeonov, Larysa Hrytsenko et al.,

new technologies to mitigate–if not entirely eradicate–the attendant risks seems to have become a matter of operational necessity rather than strategic discretion. How to proceed then, if not by contrasting fraudsters through their own arms?

3. Beyond human eyes: AI's fight against digital payment fraud

"Pour lutter contre l'abstraction, il faut un peu lui ressembler"[32], wrote Albert Camus. Behind this aphorism lies a principle readily transposable to detecting digital payment fraud: effective countermeasures require not only an understanding of the adversary, but, in certain respects, also the replication if not the partial adoption of its operational patterns. Hence, considering the shift of fraud to the virtual domain, whether in relation to the commission of the offence itself (e.g. digital payment fraud) or the means employed in its commission (e.g. using deepfakes), the fact that financial and banking actors are leveraging on AI to detect and contrast it, should not come as a surprise. As a matter of fact, it seems established that within the banking and financial sector one of the most promising application areas for AI and Machine Learning (hereafter 'ML') tools is the domain of fraud management.[33] Before examining some concrete examples of AI-based tools employed in payment fraud detection, it is necessary to establish some preliminary terminological clarifications to ensure conceptual precision in the ensuing analysis.

Hence, it is worth specifying what should be understood under the terms 'AI' and 'ML'. These two notions were masterfully synthesized, through the metaphor of a child playing with Mega Blocks, by author Maris Sekar, who offers the following characterization:

> "Artificial intelligence and machine learning are used interchangeably. It is essential to clarify what they mean. Imagine a child playing with Mega Blocks. The child makes decisions on what block goes on top of

'Who benefits from AI in money laundering in Europe: the organised criminals or the AML services?' (2025) 21(1) *Human Technology*, 222–245.

32 Albert Camus, *La Peste* (Gallimard 1947).

33 Cristina Soviany, 'The benefits of using artificial intelligence in payment fraud detection: A case study' (2018) 12(2) *Journal of Payments Strategy & Systems* 103. Cf. also for more concrete data regarding Luxembourg supporting and confirming this trend in the 'CSSF thematic review on the use of Artificial Intelligence in the Luxembourg Financial Sector' (May 2025) (n 31).

> another block. The decisions are driven through past experiences (or learning). For instance, the child knows square blocks cannot go on top of the triangle blocks after trying it several times. Here, the child's decision-making mechanism to decide which block goes next can be modeled by machine learning. If the child is replaced with a robot, then the robot as a whole becomes what is known as an artificial intelligence agent. AI consists of programming a machine to do tasks that humans typically carry out.
>
> Machine learning is divided into two main categories – *supervised learning* and *unsupervised learning*. In supervised learning, the labeled inputs and expected output of the process being modeled are used to train the model. In contrast, unsupervised learning involves the use of self-learning techniques for modeling an unlabeled dataset. In our example with the child and the Mega Blocks, supervised learning is when the child learns from their parent, showing them how to use the blocks to build a tower. Unsupervised learning is when the child learns to build a house that has never been constructed before based on their own understanding by experimenting with different constructs. The difference between supervised and unsupervised learning is an important distinction, and it will be used to explain some of the challenges of supervised learning".[34]

Analogously to the way "fraud" operates as an umbrella term for a range of illicit activities aiming at deceitfully tricking people, AI may likewise be seen as the umbrella term comprising multiple distinct subfields, one of which is ML. It is this last subfield which seems to be at the very heart of the various tools used in payment fraud detection.[35] Hence, although this contribution is not on engineering and we certainly do not possess the technical expertise to present the precise operational mechanics of these systems, it is important, for the sake of clarity, to briefly present some of their features.

---

34 Maris Sekar, *Machine Learning for Auditors. Automating Fraud Investigations through Artificial Intelligence*, (Apress 2022) 3–12.

35 Cf. notorious fraud and financial crime solutions known for being used by banking and financial institutions like Feedzai, Teradata, Ayasdi which all rely on some branches of ML to develop their AI based fraud detection tools: Feedzai, https://www.feedzai.com/ accessed 2 March 2026; Teradata Corporation, https://www.teradata.com/accessed 2 March 2026; Ayasdi, 'Delivering 100 % system compatibility for Ayasdi's ML infrastructyre' https://www.avenga.com/success/ml-solution-extracts-insights-from-data/ accessed 2 March 2026.

As already noted in Sekar's formulation, ML constitutes a subcategory of AI distinguished by its capabilities to identify patterns from a considerable amount of data, taking into account various factors, like the geographical origin of the payment authorization request, the transaction amount, or simply the frequency of the transactions. In the context of payment fraud detection, ML systems will rely on data on previous transactions, learning from them all while understanding how to distinguish a legitimate transaction from a fraudulent one. Among the various ML algorithms several types are recurrent for payment fraud detection. Decision trees and random forest algorithms,[36] for instance, are useful in classifying problems by distinguishing legitimate transactions from fraudulent ones, while deep learning algorithms will automatically extract and learn features from data.

By way of illustration–albeit in a simplified form- an AI-based fraud detection system employing deep learning algorithms will learn from the collected data and develop a behavioural profile for an individual account holder. Such a system may determine, on the basis of historical transaction data, that a given customer, for instance, typically conducts low-value payments from a consistent type of device, operating from a stable network location, and within a habitual time range. If, thereafter, a payment authorisation request for a significantly higher amount is initiated from a different type of device, via an atypical network location, and at an unusual time, the pronounced divergence from the established transaction profile would prompt the system to flag the activity as anomalous for further review. As a result, the fraud detection mechanism will flag the transaction as an out-of-the-ordinary payment hence unusual, so for the bank to review it and eventually block it.

36 For detailed studies explaining the various machine learning tools used for payment fraud detection cf. Victor Chang et al., 'Digital payment fraud detection methods in digital ages and Industry 4.0' (2022) 100 *Computers and Electrical Engineering;* Ryman-Tubb, Krause, Garn, (n 24); Vanini et al (n 24); C Chethana and Piyush Kumar Pareek, 'Analysis of Credit Card Fraud Data Using Various Machine Learning Methods', in Sita Rani et al., *Big Data, Cloud Computing and IoT Tools and Applications* (Chapman & Hall 2023).

3.1. Every rose has its thorn: On the advantages and challenges of ML payment fraud detection tools

The advantages of the use of AI based tools are certainly undeniable. Given the exponential and increasing number of digital payments,[37] the workload of processing the data has simply become inhumane especially if one considers the rapidity with which the authorisation requests need to be answered. As a result, inhumane work requires an inhumane answer, namely AI tools. Another advantage of AI tools, in particular ML ones, is their ability to learn and rapidly adapt to new fraud's techniques. Yet, once again, new opportunities go hand in hand with new challenges. In other words, despite the visible advantages of these AI tools, some issues still need to be addressed and ideally resolved.

It goes without saying that purchasing these AI tools comes at a significant cost for the banks, especially if one considers the fact that they are not, at least in the vast majority of cases, supposed to replace the humans who will still need to be placed in the loop. Yet, it seems to us that the argument of the cost of these tools is not a convincing one. As a matter of fact, a valid counterargument is to replicate that the costs of not detecting fraud are definitely much higher. This is particularly true within the EU where under article 73 of the PSD2, payment service providers can be held liable in case of unauthorised payment transaction[38] and will have to, except in some exceptional cases, reimburse the unauthorised payment transaction.

---

37 Cf. for some statistics on this matter: Committee on Payments and Market Infrastructures, 'Tap, click and pay: how digital payments seize the day', Brief n°3 (February 2024).

38 It should be noted that the border between authorised and unauthorised payment might become quite blurred in the context of digital fraud. Take for example the case of a CEO fraud which technically is committed with the consent of the victim who actually authorizes the transaction because of the fraudster's deceitful means who presents himself/herself as, in this case, the CEO. To address these new issues arising from new fraud forms, the future third directive on payment services (PSD3) is supposed to go beyond the PSD2. Cf. for more details on the subject: Emanuel van Praag, 'Authorised Push Payment Fraud: Suggestions for the Draft Payment Services Regulation' (2025)190 *European Banking Institute Working Paper Series* https://ssrn.com/abstract=5241100 or http://dx.doi.org/10.2139/ssrn.5241100 accessed 7 August 2025. Cf. also for life updates on the revision schedule: European Commission press release on 'Modernising payment services and opening financial services data: new opportunities for consumers and businesses' https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543 accessed 17 July 2025. European Parliament – Legislative Train Schedule, 'Revision of EU rules on payment services', at the following link:

Another challenge, that applies to the use of AI in general, is the feared black-box effect[39] which pertains to the opacity of the latter's results. Indeed, the difficulties in understanding and assessing the accuracy hence the reliability and validity of the results generated by AI tools often prove to be problematic. Clearly, explainability is a sensitive topic, especially since it is legitimate for customers to require their banks to explain how and why a specific AI tool has taken a given decision. Nonetheless, we think that the black-box issue proves, for a series of reasons, to be less problematic in the framework of fraud detection tools. On the one hand, one should consider that although blocking a transaction because it is suspected to be fraudulent represents a sort of "interference with a person's free will", in the sense that in case of a false positive a legitimate transaction will not be authorized, it is not the most invasive decision that one can take toward an individual.

In contrast, one should think of decisions taken after relying on AI tools' results in the field of criminal law for instance. In this case, explaining how and why the AI tool reached a given conclusion upon which the law enforcers have relied on, will prove not only crucial in order to be used as evidence but also essential to preserve the defense rights. A scenario that does not fit the case of payment fraud detection, especially if one considers that, at the end of the day, not authorizing a transaction because it seems fraudulent is a precautionary act to spare the customer from a potential harm (and in some sense also the bank itself which under the PSD2 would eventually need to reimburse the lost sum). An act that seems to perfectly fit the "better safe than sorry" motto. What is more, one should not forget that blocking a transaction is not an irreversible decision. A customer whose digital payment request was refused can always ask for the reasons that led to such a refusal and, once proven that the former was a legitimate one coming from herself/himself, the transaction can be flagged as legitimate and, hence, authorized.

A more complex and perhaps the true Gordian knot when it comes to the use of ML for payment fraud detection is without any doubt the gathering and use of data. As already mentioned, a common point between

---

https://www.europarl.europa.eu/legislative-train/theme-an-economy-that-works-for-people/file-revision-of-eu-rules-on-payment-services accessed 17 July 2025.

39 Cf. for more details on the black-box issues: Chinu, Urvashi Bansal, 'Explainable AI: To Reveal the Logic of Black-Box Models' (2024) 42 *New Generation Computing*, 53–87; Luke Tredinnick and Claire Laybats, 'Black-box creativity and generative artificial intelligence' (2023) 40(3) *Business Information Review*, 98–102.

the various ML algorithms is the fact that they need to learn through data which, in this case, are nothing else than historical figures and information from previous existing experiences with regard to payment transactions and payment frauds. As rightly stressed out by several scholars "the fraudster behaves differently during a payment transaction than the account owner and/or the payment has unusual characteristics, such as an unusually high payment amount or transfer to an account in a jurisdiction that does not fit the life context and payment behavior of the customer. […] fraud in online payments can only be detected based on individual data, as such fraud can only be detected through the possible different behavior of the fraudster and the account holder during payments. As fraudsters learn how best to behave undetected over time, they adapt their behavior".[40] As a result, the quality as well as the quantity of the data used to train the algorithms proves to be vital if one wants to continue using them.

Against this background, a first strain of challenges which will only be briefly mentioned concerns the gathering of data and the privacy issues. It is important to note that training ML algorithms not only requires the gathering of large amount of data but will also touch upon more private and sensitive information such as an individual's transaction history. To overcome the privacy issues, one could rely upon the exclusive use of synthetic data.[41] Yet, even the latter will need some original data to be trained and furthermore, it is not clear whether they can cover and outperform data stemming from concrete and existing experiences. Nonetheless, one should not forget when it comes to payment fraud detection, that under article 94 PSD2, payment service providers and payment systems are explicitly allowed to process personal data to, notably, prevent and detect payment fraud. This same provision specifies that such processing and gathering will have to be limited to the scope of payment services and that it will require the consent of the user. Also, article 94 PSD2 refers to the general provisions of directive 95/46/EC, which was repealed and replaced by the General Data Protection Regulation (in short 'GDPR')[42], that will

40 Vanini et al (n 24).

41 Cf. for more details on the use of synthetic data for AI tools: Fernando Lucini, 'The real deal about synthetic data' (2021), *MIT Sloan Management Review,* at https://sloanreview.mit.edu/article/the-real-deal-about-synthetic-data/ accessed 2 March 2026; Vincent Granville, *Synthetic data and generative AI* (Morgan Kaufmann Elsevier 2024); Khaled El Emam, *Accelerating AI with Synthetic Data* (O'Reilly 2020).

42 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

have to be applied by the providers gathering the data. Hence, without having to dwell into details of the GDPR requirements, let us highlight the main rules set out in the GDPR that need to be complied with by the implicated collecting entities. More to the point, pursuant to the GDPR, the consent to process the data (article 7), which shall be done in a lawful and transparent manner (article 5), communicating the specific information to the users at the moment they collect their data (articles 12 and 13) all while pursuing a specific and legitimate purpose (article 6) will have to be complied with. In the framework of digital payment fraud, *i.e.*, a clear case of crime prevention, the issue of gathering sensitive data, will be mostly dealt and complied with. Yet is gathering and processing data sufficient in the context of fraud detection through ML tools?

3.2. Sharing is caring?

The privacy preservation resurfaces with regard to another challenge pertaining to data gathering, namely the possibility to share them among banks to foster the identification of fraud patterns. It is already worth noting that under the GDPR sharing data with third parties is not prohibited, as long as the sharing is done in compliance with its provisions, notably that it is performed with the consent of the users, in this case the bank customers.[43] A consent which does not seem impossible to obtain. As demonstrated by Comply Advantage, one of the leading firms proposing AI tools for financial crime detection, including fraud, 65 percent of the surveyed customers were open to the idea of banks sharing their transactional details among themselves in order to foster the identification of fraud patterns.[44] Also, one could rely on the fact that there are currently new methods that are being developed to share data all while preserving privacy,

data and on the free movement of such data, and repealing Directive 95/46/EC, OJL 119/1.

43 Cf. articles 5(1); 6(4) and 89(1) as well as recitals 39 and 50 of the GDPR.

44 Comply Advantage, 'Technology is creating new fraud frontiers – but consumers don't want AI to protect them' https://complyadvantage.com/press-media/technology-is-creating-new-fraud-frontiers-but-consumers-dont-want-ai-to-protect-them/ accessed 15 August 2025.

which use so-called "privacy-preserving record linkage (PPRL)", able to hide personally identifiable information.[45]

As a result, a crucial and turning point in having the best working ML tools is the ability to rely on qualitative data to train the algorithms. In fact, as pointed out by some authors, one of the main challenges with ML tools is the quality of the data used to train the models.[46] Going back to Sekar's metaphor, just like a child who is provided with a bad education, if one provides AI with "bad" or so-called "dirty" data, *i.e.*, data which contain errors or are missing some specific values, the algorithm will absorb and learn from these data ending up providing unreliable and wrong interpretations. The importance of reliable data is also stressed out by Interpol, according to which to foster the prevention and contrast payment fraud through the use of AI tools the efforts should be concentrated into "strengthen data collection and analysis on financial fraud in order to develop more informed and effective counter strategies".[47] Against this background, a legitimate question arises, is there a way to obtain the highest-quality possible data to train the various algorithms?

Relying on the "unity makes strength" motto, the response to the question might lie in the acknowledgment that detecting payment frauds could be improved through the sharing of data among banks.[48] After all, which better way to get the whole picture of payment fraud than by adding and equating various experiences with the latter, just like for solving a puzzle, to get the whole picture you will have to manage to put all the pieces together. Nonetheless, if the solution is so straightforward, why do banks still miss out on this opportunity, or at least do not sufficiently profit from it? Especially if one relies on the already mentioned recent Comply Advantage survey which showed a high consent rate among customers to share their data among banks to prevent fraud. After all, detecting and fighting fraud, including digital payment one, is an issue already tackled, at

45 Cf. Satish Thomas and James Sluss, 'Fraud detection through data sharing using privacy-preserving record linkage, digital signature (EdDSA), and the MinHash technique: Detect fraud using privacy preserving record links' (2023) *The Journal of Engineering*.

46 Sekar (n 34).

47 Interpol (n 12).

48 Kaushikkumar Patel, 'Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques' (2023) 71(10) *International Journal of Computer Trends and Technology*, 69–79; Vanini et al (n 24); Basel Committee on Banking Supervision, Discussion Paper (n 26).

least from the criminal law dimension, at the EU level through the directive on combating fraud and counterfeiting of non-cash means of payment,[49] which requires Member States to set up, among others, criminal law measures for digital payment fraud (articles 3 to 6) all while providing penalties for natural persons (article 9) and a liability system for legal persons (article 10). Interestingly enough, this same directive foresees under its article 18 the establishment of a monitoring programme through the collection of data and other evidence. Its second paragraph specifies that Member States will have to put in place a system "for the recording, production and provision of anonymised statistical data measuring the reporting, investigative and judicial phases"[50] of the various fraud offences.

An argument that could be instinctively raised in opposition to such a large-scale data sharing and collection is the one arising from the risk related to data breaches and cyberattacks. Nonetheless, without underestimating this risk, one should not forget that, at least within the EU, the regulation on digital operational resilience for the financial sector (in short 'DORA')[51] was introduced precisely to strengthen the resilience of digital operations within the financial sector by creating a common information and communication technology risk management framework. Also, the regulation itself foresees under its article 45 the possibility and the conditions for financial entities to exchange cyber threat information and intelligence among themselves. Furthermore, whether by sharing data or not, banks, among others, will sadly but inexorably always be threatened by the risk of cyberattacks and data breaches, so that invoking this argument to oppose data sharing on payment fraud seems unconvincing.

What seems more convincing given the goals of the banks and the ineluctable competition spirit between them, is the fact that banks do not necessarily have an interest to share these data. Certainly, one could say that by sharing their data they will improve their own algorithms by gaining new data to train the latter. Yet, it seems safe to affirm that the biggest

49 Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, OJ L123/18.

50 Article 18 of the Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, OJ L123/18.

51 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011, OJ L333/1.

banks are probably the ones with the largest database. Why should they share data on their customers with other smaller banks or, even worse, with direct competitors, *i.e.,* other significant banks? Is there a way of addressing the issues with the gathering and sharing of data? Could it be possible to set up a centralized database?

This idea might seem unreasonable, almost heretical at first sight. Yet, it relies on the fact that data sharing and especially the collection of data within a centralised entity is not a novelty, even when it comes to the fight against fraud. We are referring to the current centralised databases within the EU for fraud detection against EU funds, like the 'ARACHNE risk scoring tool'[52] based on data mining exploiting, both internal and external data, and which was put in place as a management verification for the European Structural and Investments Funds to detect, among others, frauds in the context of their activities. Also, the EU enjoys the benefits of the 'EDES' database[53], containing a list of persons that are excluded from contracts financed through EU funds, *inter alia*, because of fraud. A reliance on AI solutions that will certainly increase within the next years, as revealed by the Commission in its Anti-Fraud Strategy Action Plan where one of the themes is "Foster digitalisation and the use of IT tools to fight fraud".[54]

52 Cf. for more details on the functioning of the ARACHNE risk scoring tool the dedicated website at the following link: https://ec.europa.eu/social/main.jsp?catId=325&intPageId=3587&langId=en accessed 13 November 2024. Cf. also the publicly available European Commission's Charter for the introduction and application of the ARACHNE risk scoring tool in the management verifications, where it is possible to read that the tool "*is based on internal and external data. These internal data (projects, beneficiaries, contracts, contractors and expenses) are extracted by the managing authority from their local computerized systems and uploaded on a dedicated server of the Commission services. External data are provided by two external service providers […]. The first database contains financial data as well as shareholders, subsidiaries and official representatives of over 200 million companies. The second database is composed of a list of politically exposed persons, sanction lists, enforcement lists and adverse media lists*", 4–5.
European Commission, *Arachne Charter for the introduction and application of the Arachne risk scoring tool in the management verifications* (1st January 2024). https://employment-social-affairs.ec.europa.eu/document/download/a43cb969-8a8d-492b-b1c6-938edfb1f63a_en?filename=Arachne-Charter.pdf accessed 3 March 2026.

53 Cf. for more details on the functioning of the EDES database: https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures/edes/edes-database_en. accessed 13 November 2024.

54 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee

After all, the idea of creating a centralized database at EU level, at least within the Eurozone, seems also the next logical step to an already, some sort of existing, data gathering process. We are referring to the reporting approach foreseen by the PSD2, more precisely under its article 96(6) according to which payment service providers are required to provide the EBA and ECB with statistical data on fraud relating to different means of payment on an annual basis at least. Hence, a considerable amount of data is already gathered by these authorities. Of course, the question will be on the type of data it gathers. In contrast to the reporting under the directive of combating fraud, whose article 18(3) sets as a limit data on the number of offences related to fraud and the number of prosecuted and convicted persons, the data gathered under article 96(6) PSD2 seem more far reaching. Indeed, having a look at the already mentioned recently published EBA and ECB report on payment fraud, one can see the different categories under scrutiny, namely the levels of payment fraud (*i.e.*, the total value of fraudulent transactions reported) as well as the losses due to the latter, the different and main types of fraud, a more detailed study on the transactions authenticated or not through the strong customer authentication, the geographical dimension of payment fraud, as well as a country-by-country review on payment fraud. A rich variety of topics that gives an idea of the amount of data that is already reported, collected and within the hands of the ECB and EBA. Hence, considering the fact that EBA has already launched a EU's central database for anti-money laundering and counter-terrorism financing (*EuReCA*),[55] could a similar database with relevant data for fraud detection, accessible to the various banks, be a viable and useful in the banking context, by offering ML tools and more particularly their algorithms the best education possible? *Affaire à suivre.*

Conclusion

In an era where the use of new technologies has simplified the traditional banking services for the customers, to the point where through a simple

of the Regions and the Court of Auditors: Commission Anti-Fraud Strategy Action Plan (2023 revision)' (2023).

55 For more details on the new EuReCA Database, cf. EBA's dedicated webpage on the subject at the following link: https://www.eba.europa.eu/regulatory-technical-standards-central-database-amlcft-eu. accessed 13 November 2024.

click or by using a card, if not even a phone, they can proceed to cashless payments, it had to go without saying that new forms of risks would arise. Between friend and foe, these technologies, nowadays often based on AI, have become a daily reality just like digital payment fraud. To respond to these new risks, banks are increasingly leveraging AI tools, especially those based on ML technology, to prevent and detect fraud, particularly payment fraud.

And, if it goes without saying that the fight against fraud will be an eternal one, as witnessed by the fact that it exists since basically the beginning of History, to the point that it is quite safe to say that humanity will probably never get rid of it, it is also true that there might be solutions to efficiently contrast it or at least facilitate its detection. ML based tools have proven a necessary and useful ally in this eternal fight, yet, as rightly said by some authors: "AI requires the capability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent human beings: the ability to reason, finding out meaning for specific concepts, generalization from examples or learning from past experiences to make smart decisions in new (unseen) situations. The smart decisions in AI applications rely on the outputs of the learning process".[56]

While filtering bad from good data will remain within the hands of various engineers, the legal field could contribute by facilitating if not imposing the access to qualitative and quantitative significant data. A potential solution or at least a suggestion, fostering the sharing between banks, if needed through the establishment of a centralized datacenter.

56 Soviany (n 33) 102.