PAYMENT FRAUD IN ITALY AND IN IN THE UK: COMPARATIVE ANALYSIS AND PROSPECTS FOR REFORM

GIOVANNI BATTISTA BARILLÀ
Professore associato
nell'Università di Bologna

SUMMARY: 1. Digital payment fraud and COVID-19 pandemic. – 2. From unauthorised to authorised fraud: rise in app fraud. – 3. Comparative analysis of payment fraud statistics in Italy and the UK. – 4. Payment fraud overview. – 5. Managing compliance expenses. – 6. UK legal framework. – 7. Corporate criminal liability and "failure to prevent fraud". – 8. PSR's APP fraud reimbursement requirement. – 9. Gross negligence as the customer standard of caution. – 10. Italian legal framework. – 11. New EU rules on payment fraud. – 12. Conclusion. [1]

1. – Comparing payment fraud rates across different countries is challenging due to the underreporting of fraud incidents and the use of different parameters. However, the Social Market Foundation (SMF) discovered that, when compared to other European countries, pre-pandemic, the UK had the highest rate of card fraud victims per 1000 persons and suffered the greatest financial losses, with Italy having significantly lower averages than its EU counterparts [2]. The UK has emerged as a particularly attractive target for digital payment fraud due to various long-term factors – globalisation, its status as an English language hub, rapid digitisation, and short-term ones – the COVID-19 pandemic, the ongoing cost of living crisis, the emergence of crypto assets, and the UK's early adoption of the Faster Payments Service (FPS) [3] [4]. This trend is not confined to the UK alone. European countries, including Italy, have experienced increasing digital payment fraud, albeit with a slight time delay compared to the UK.

[1] The opinions of experts in the banking world are quoted anonymously.

[2] R. KAPOOR, *UK Is Card Fraud Capital of Europe* (*Social Market Foundation*, 3 August 2022), https://www.smf.co.uk/uk-is-card-fraud-capital-of-europe-think-tank.

[3] The Faster Payment Service (FPS), launched in 2008 and operated by Pay.UK, allows individuals with UK bank accounts to send money to almost any other UK account, enabling near-instantaneous transfers 24/7.

[4] Pay.UK, *Faster Payment Service Principles* (2023) Version 7.6, 31/01/2023 https://www.wearepay.uk/wp-content/uploads/2023/02/Pay.UK-Faster-Payments-Service-Principles.pdf.

During the pandemic, there was a notable surge in fraudulent activities, driven by the increased usage and greater exposure of customers to digital services. However, the banking sector managed to perform well by implementing various initiatives to mitigate and tackle the rising fraud and cyber threats.

While digitalisation has been progressing rapidly over the last two decades, the COVID-19 pandemic served as a catalyst for the proliferation of payment fraud and significantly impacted consumer behaviour. Fraud rates rose during lockdowns and the pandemic created an environment ripe for fraudsters to exploit, particularly with new-to-digital consumers and increased vulnerabilities and anxieties. The consequences of the pandemic are expected to have a lasting effect due to the adoption of changed habits, and a return to pre-pandemic norms is improbable [5].

2. – Recently, there has been a significant and exponential rise in authorised fraudulent transactions, often referred to as «scams». This transition from unauthorised to authorised fraud, initially observed in the UK and subsequently in Italy and other European countries during the pandemic, presents a challenge due to the widespread use of sophisticated social engineering tactics, in contrast to the more conventional and consolidated unauthorised fraud practices [6].

In recent times, there has been a notable transition, not only during the pandemic but also predating it in the UK, where the focus has shifted from actual fraud to scams, making scams the predominant occurrence. This trend towards scams is also evident in both the European and Italian contexts [7].

One of the most prevalent forms of authorised payment fraud is known as Authorised Push Payment (APP) fraud, relying heavily on social engineering techniques, as detailed in the upcoming chapter's case study on emerging tactics. It involves manipulating individuals or businesses into sending money or sensitive information to criminals who impersonate legitimate payees, leading the victims to unwittingly authorise fraudulent transfers [8]. APP fraud has significant repercussions within the banking sector, as it hinges on deceiving victims into transferring funds under false pretences: sending money to a different recipient or for a different purpose

[5] M. LEVI, R. G. SMITH, *Fraud and Pandemics*, (2022) 29, Journal of Financial Crime, https://doi.org/10.1108/JFC-06-2021-0137.

[6] HM Government (n 2).

[7] Interview Head of Cybersecurity ID, Italian Bank.

[8] FCA HANDBOOK, https://www.handbook.fca.org.uk/handbook.

than what the victim initially believed[9]. Although APP fraud data has started to be collected relatively recently, in 2017, the trends over time indicate that this type of scam is experiencing exponential growth, worsened by the COVID-19 pandemic and the use of faster payments [10].

Detecting and preventing APP fraud poses significant challenges. As Jordanoska documented, warning signs that a customer may be falling victim to an APP scam include rapid transactions occurring within a brief timeframe, originating from a seldom-used bank account with minimal prior withdrawals. While the obstacles in thwarting and identifying these scams stem from various factors. These encompass the underlying social engineering tactics used to manipulate victims, the voluntary nature of the victim's actions within the scam, the increasing complexity of scam scripts, and the proliferation of real-time and expedited payment systems that facilitate substantial fund transfers with limited scrutiny [11].

3. – This section analyses payment fraud dynamics in Italy and the UK, primarily using the latest available data from 2022 to identify similarities and differences in their fraud trends, suggesting that Italy is following the UK's main fraud patterns, albeit with a slight time delay. Understanding the vulnerabilities exploited by fraudsters in each country enables more effective resource allocation for defensive mechanisms, but year-on-year comparisons have limitations as they provide snapshots rather than comprehensive depictions of the intricate fraud dynamics [12].

In the UK, a comprehensive dataset on fraud incidents is compiled from the National Fraud Intelligence Bureau (NFIB), which gathers information through Action Fraud, Cifas, and UK Finance, ensuring robust data triangulation. On the other hand, Italy primarily relies on the annual CERTFin report [13], with additional minor contributions from public bodies like UCAMP [14] within the Ministry of Economy and Finance (MEF)[15]. At the

[9] PSR, *APP Scams*, (August 2023), https://www.psr.org.uk/our-work/app-scams/.

[10] A. JORDANOSKA, *The Management of Financial Crime Risks by Financial Technology Companies (FinTechs)*, Unpublished Extended Project Report (2022).

[11] A. JORDANOSKA, ibid.

[12] M. LEVI, *Written Evidence (FDF0042)*, 2022, https://committees.parliament.uk/writtenevidence/108054/pdf/.

[13] The writer acknowledges the Italian CERTFin for generously sharing their latest payment fraud reports, typically restricted to members.

[14] The Italian Central Means of Payment Antifraud Office (Ufficio Centrale Antifrode dei Mezzi di Pagamento).

[15] MEF UCAMP, *Rapporto statistico sulle frodi con le carte di pagamento 2021*, n. 11/2021,https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/antifrod

European level, the European Central Bank (ECB) and the European Payments Council also issue annual reports on card fraud and payment threats. The UK possesses richer and more diverse data for cross-referencing, yet non-comparable parameters and varying focus on different fraud sectors often create a confusing overall picture, while Italy's more straightforward and less scattered fraud data landscape lacks cross-referencing.

More fraud data is always valuable, but concerns continue about its reliability, due to self-reporting and underreporting, and sector-specific stats resulting in gaps, biases, and a fragmented fraud landscape. Comprehending the issue's magnitude and its enabling factors remains elusive, necessitating reliance on anecdotal rather than statistical evidence [16].

4. – In 2022, the fraud landscape in Italy and the UK indicates a return to pre-pandemic levels, suggesting pandemic-related spikes in fraud incidents may have been temporary rather than lasting shifts in underlying trends. Italy experienced its most successful year in combating payment fraud in 2022 since before the pandemic, with the CERTFin report [17] indicating a reduced number of "finalised" frauds when comparing 2022 to 2021 (down by 6% in quantity and 8% in amount). In Italy, the Retail segment remains disproportionately affected by fraudulent transactions, constituting about 95% of the total, of which 65% authorised fraud. Whereas in the Corporate sector, unauthorised fraud accounted for 62% of cases. Finally, in a European context, Italy consistently maintained a lower card fraud rate than the Single Euro Payments Area (SEPA) average, while the UK often surpassed it [18].

Our bank aligned with findings from the Italian 2023 CERTFin report and worldwide trends in fraud. During the pandemic, fraud escalated in scale and frequency. The banking industry reacted with anti-fraud protocols, yielding significant post-pandemic reductions in attacks.

The Crime Survey for England and Wales (CSEW) for the year ending March 2023 revealed a total of 3.65 million fraud offences (40% of total crime

e_mezzi_pagamento/antifrode_mezzi_pagamento/Rapporto-statistico-sulle-frodi-con-le-carte-di-pagamento-edizione-2021.pdf.

[16] Interview Financial Crime Expert, Think Tank.

[17] CERTFin (n 3).

[18] BANCA D'ITALIA, *Le frodi con carte di pagamento: andamenti globali ed evidenze empiriche sulle frodi online in Italia*, https://www.bancaditalia.it/pubblicazioni.

in the UK) [19]. When compared to 2021, 2022 UK's payment fraud losses decreased by 8%, while fraud cases by 4%, with a shift towards authorised fraud (54% of the total in 2022) [20]. Cifas data revealed a significant 68% of all fraud cases as identity fraud in the UK in 2022, alongside notable increases in advance fee fraud, misuse of facilities and false application fraud [21].

a) Fraud Vectors

In 2022, communication channels, primarily phone calls and SMS, accounted for nearly 70% of cases in Italy. Retail customers face 90% of fraud through customer manipulation (authorised fraud), while corporate customers encounter Business Email Compromise (BEC) in nearly half of all fraud cases [22]. Shifting to the UK, online sources drive 78% of fraud cases, mainly lower-value purchase scams, accounting for 36% of total losses. Meanwhile, telecommunications account for 18% of cases, typically involving higher-value impersonation scams, contributing to 44% of total losses [23].

b) Fraudulent Payment Types

In both Italy and the UK, instant payments take centre stage in 2022 due to their operational attributes. In Italy's Retail sector, SEPA Instant Credit Transfer (SCT) is implicated in over 40% of fraud cases, with an even higher percentage in the corporate sector (70%) [24]. Turning to the UK, in 2022 Faster Payments accounted for 98% of APP fraud cases, with mobile banking as the dominant payment channel (59% of volume) [25].

c) Victim Demographics

[19] *ONS Crime in England and Wales: Year Ending March 2023*, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023.

[20] *UK Finance 2022 Annual Fraud Report*, https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf.

[21] CIFAS Fraudscape 2023, https://www.fraudscape.co.uk/.

[22] CERTFin (n 3).

[23] UK Finance (n 54).

[24] CERTFin (n 3).

[25] UK Finance (n 54).

In 2022, in Italy's Retail sector, the age group 45-60 years emerges as the most affected (30%), followed by those aged 30-35 (27%) and over 60 (26%), while the under-30 cohort experiences the least impact (17%) [26]. In the UK, in 2022, individuals constitute 88% of fraud victims [27], younger demographics aged 20-39 stand out as particularly vulnerable to fraud and those aged 21-25 are more at risk of impersonation scams [28]. In the UK, victims with disabilities and social renters face heightened vulnerability to fraud.[29] The emotional toll of fraud is profound, with nearly three-quarters of victims reporting emotional distress, highlighted by Action Fraud receiving over 300 calls annually from individuals at risk of suicide due to fraudulent activities [30]. Studying fraud victim demographics is crucial for defining «vulnerability» parameters, as exemplified in the UK, where it serves as a mitigating factor for banks reimbursing authorised fraud victims.

d) Insight: Cybersecurity

While DDoS attacks are not directly a form of payment fraud, they can be part of a broader cybercriminal strategy that includes fraudulent financial activities targeting banks. In 2022, 57% of surveyed banks in Italy detected and mitigated 413 DDoS attacks, influenced by the Russia-Ukraine conflict, which fuelled "hacktivism", particularly by pro-Russian groups Killnet and NoName057. Although 22% of banks recorded DDoS attacks linked to these groups, none were deemed "serious". Furthermore, 83% of Italian banks identified dependencies on "End-of-Life" (EOL) IT components, with 50% having dependencies on EOL client components and 72.2% on EOL server components.[31] In H1 2022, the UK financial sector saw a significant rise in DDoS attacks, with more incidents reported to the Financial Conduct Authority (FCA) in March and April than in the entire year of 2021 [32]. The

[26] CERTFin (n 3).

[27] *NFIB Fraud and Cyber Crime Dashboard*, https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46.

[28] UK Finance (n 54).

[29] ONS, *Nature of Fraud and Computer Misuse in England and Wales: Year Ending March 2022*, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022.

[30] HM Government (n 2).

[31] CERTFin (n 3).

[32] FINEXTRA, *UK Finance Suffers Surge in DDoS Attacks* (*Finextra Research*, 14 September 2022), https://www.finextra.com/newsarticle/40955/uk-finance-suffers-surge-in-ddos-attacks.

group Killnet caused disruption, targeting UK entities like the Bankers Automated Clearing Service (BACS), the London Stock Exchange (LSEG), and the Prince of Wales's official website as retaliation for the UK's stance on Ukraine [33].

5. The banking sector is among the most heavily regulated industries, and for PSPs operating within the regulatory perimeter, compliance expenses often exceed the losses caused by fraud [34]. This can be attributed to the fact that the recorded loss primarily reflects operational costs and fails to capture the not quantifiable reputational damage, that can have long-lasting effects on customer trust and the bank's brand image.

Insufficient investment in protective systems, left static over time, leads to an exponential surge in fraudulent activities. The growth of fraud tends to follow an exponential trajectory, whereas the reduction in fraud usually progresses linearly in response to the bank's implemented measures [35].

Investing proactively in compliance not only mitigates current losses but also helps prevent potential future financial setbacks, as seen with the example of the interviewed Italian Bank heavily investing in Artificial Intelligence (AI), despite not experiencing AI-driven fraud cases so far [36]. Attempting to directly compare compliance expenses with fraud losses does not yield meaningful insights, as these two elements operate under vastly different logics, dynamics, and trends. Each necessitates a distinct approach and understanding, given their unique nature and implications [37].

The dynamics of fraud and compliance present stark contrasts. Fraud incidents exhibit numerous spikes, whereas compliance costs remain stable and predictable [38].

In 2022, UK financial services spent around £34.2 billion on complying with financial crime regulations, comparable to 75% of the UK's 2021/22

[33] A. SCROXTON, *Killnet DDoS Hacktivists Target Royal Family and Others* (*ComputerWeekly*, 22 November 2022); https://www.computerweekly.com/news/252527560/Killnet-DDoS-hacktivists-target-Royal-Family-and-others.

[34] LEXISNEXIS RISK SOLUTIONS, *True Cost of Compliance 2023 Report - Is the UK Financial Services Sector Doing Enough of the Right Things to Effectively Fight Financial Crime?*

[35] Interview Head of Anti-Fraud, Italian Bank.

[36] Interview Head of Cybersecurity ID, Italian Bank.

[37] M.T. BIEGELMAN and J. T. BARTOW, *Executive Roadmap to Fraud Prevention and Internal Control: Creating a Culture of Compliance*, London, 2012.

[38] Interview Head of Cybersecurity ID, Italian Bank.

defence budget [39]. The average UK firm spent £194.6 million on financial crime compliance, with smaller firms disproportionately shouldering compliance costs due to their lack of economies of scale. However, the impact varies among different financial sectors, with retail, commercial, and investment banks facing higher costs compared to the average, while neobanks experience lower costs. Compliance spending has been rising since 2020 and is expected to continue increasing, with the highest allocations in the next three years going toward transaction monitoring, Know-Your-Customer (KYC), and onboarding fraud checks [40].

6. – When examining the UK fraud landscape, a multitude of legislations emerge as significant, prompting the reference to a '*panoply of laws*' [41]. The key legislative tools are briefly outlined below, but the primary emphasis centres on two recently introduced UK initiatives: (i) the HM Government Fraud Strategy, published in May 2023 [42], and (ii) the Payment Systems Regulator (PSR)'s new APP fraud reimbursement requirement, announced in June 2023 [43]. These initiatives have been received by the payments industry and customers with contrasting opinions, and this study seeks to evaluate their effectiveness by incorporating observations from expert interviews. Finally, the Integrated Review (IR) Refresh 2023 [44] designated fraud in the UK as a «national security threat», and the Royal United Services Institute (RUSI) has highlighted instances where fraud has financed terrorist endeavours [45].

[39] MINISTRY OF DEFENCE, *MOD Departmental Resources: 2022*, https://www.gov.uk/government/statistics/defence-departmental-resources-2022/mod-departmental-resources-2022.

[40] LEXISNEXIS RISK SOLUTIONS (n 88).

[41] SOCIAL MARKET FOUNDATION, *Written Evidence (FDF0026)*, 2022, https://committees.parliament.uk/writtenevidence/108022/pdf/.

[42] HM Government (n 2).

[43] PSR, *PS23/2 Fighting APP Fraud: A New Reimbursement Requirement. Response to September 2022 Consultation* (CP22\4), 2023; https://www.psr.org.uk/media/iolpbw0u/ps23-3-app-fraud-reimbursement-policy-statement-final-june-2023.pdf.

[44] *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World*, https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

[45] H. WOOD and others, *The Silent Threat: The Impact of Fraud on UK National Security* (RUSI 2021), https://static.rusi.org/the_silent_threat_web_version.pdf.

Fraud was labelled a «national security» concern predating the pandemic, and this stance remains pertinent and unchanged. If anything, the threat might have expanded, potentially involving state actors and connections to cryptocurrency fraud.

a) Overview of UK Measures

(i) Computer Misuse Act 1990 [46]: This legislation addresses computer-related offences with key offences: unauthorised access to computer material (Section 1), unauthorised access with intent to commit or facilitate the commission of further offences (Section 2), and unauthorised acts impairing computer operation (Section 3). Calls for its review have arisen to align it with '*where we are now*' [47].

(ii) Fraud Act 2006 [48]: The Fraud Act modernised and clarified fraud laws, serving as the primary legal tool for prosecuting fraud. It identifies three means of committing fraud: false representation (Section 2), failure to disclose information (Section 3), and abuse of position (Section 4). While well-constructed, its effectiveness is hampered by application challenges and deficiencies in fraud prevention and enforcement.[49]

(iii) Data Protection Act 2018[50]: Incorporating the EU General Data Protection Regulation (GDPR)[51] into UK law, this Act governs the use of personal data. The House of Lords has advocated for the Information Commissioner's Office (ICO) to foster a permissive approach, or «safe harbour», for private sector data sharing to combat fraud [52].

(iv) Telecommunications (Security) Act 2021 [53]: This legislation addresses the historical issue of fraud facilitated through telecom services, obliging providers to manage security risks and mitigate breaches.

(v) Proceeds of Crime Act 2022 [54]: POCA provides the legal framework for freezing and confiscating unlawfully acquired assets and criminal proceeds.

(vi) Financial Services and Markets Act 2023 [55]: FSMA empowers regulatory oversight for reimbursement in APP fraud cases, extends regulation to

[46] Computer Misuse Act 1990.

[47] P. SMITH, *Corrected Oral Evidence*, 2022; https://committees.parliament.uk/oralevidence/10178/html/.

[48] Fraud Act 2006.

[49] HOUSE OF LORDS, *Fighting Fraud: Breaking the Chain. Report of Session 2022-23*, 2022; https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf.

[50] Data Protection Act 2018.

[51] General Data Protection Regulation (GDPR) (EU) 2016/679.

[52] House of Lords (n 109).

[53] Telecommunications (Security) Act 2021.

[54] Proceeds of Crime Act 2002.

specific crypto-assets and alters the authorisation procedures for financial promotions.

Upcoming Bills on Counter-Fraud Policy:

(i) *Online Safety Bill 2021* [56]: It mandates large online platforms hosting user-generated content (Category 1) and search engines (Category 2A) to prevent fraudulent paid advertisements (a sort of duty of care in clauses 34, 35, and 36). The House of Lords recommended enhancing anti-fraud efforts by extending prevention measures to all platforms through a risk-based approach, departing from size-based criteria [57].

(ii) *Economic Crime and Corporate Transparency Bill 2022* [58]: Strengthens Companies House, enables crypto-assets seizure, and enhances information sharing to combat economic crime. The Economic Crime (Transparency and Enforcement) Act 2022 received royal assent in March 2022.

(iii) *Digital Markets, Competition and Consumer Bill 2022-23* [59]: Aims to counter fake online reviews, increase competition by regulating Tech firms, empower the Digital Markets Unit (DMU) and strengthen the Competition and Markets Authority (CMA).

(iv) *Data Protection and Digital Information Bill 2022-23* [60]: Aims to revamp the UK data protection system and includes measures for facilitating information-sharing agreements. Currently, the Bill's progress is halted, and the Government has signalled its plans to substitute GDPR "*with its own system*" [61]. The House of Lords suggested incorporating «fraud» as a specified crime in Section 5(a) to improve transparency [62].

While identity theft, extensively employed by fraudsters, is often the precursor of payment fraud, it is not a criminal offence [63]. In 2023, the Government announced no plans for a new identity theft criminal offence, as existing laws like the Fraud Act 2006 and the Data Protection Act 2018 safeguard individuals' personal data and prosecute identity theft-enabled

[55] Financial Services and Markets Act 2023.

[56] Online Safety Bill 2021.

[57] House of Lords (n 109).

[58] Economic Crime And Corporate Transparency Bill.

[59] Digital Markets, Competition and Consumers Bill.

[60] Data Protection and Digital Information Bill.

[61] S. RAVIKUMAR, W. JAMES, *Britain to Replace GDPR Data Privacy Regime With Own System*. *Reuters* (3 October 2022), https://www.reuters.com/legal/litigation/britain-replace-gdpr-data-privacy-regime-with-own-system-2022-10-03/.

[62] House of Lords (n 109).

[63] Cifas (n 55).

crimes [64]. The Government should consult on the introduction of this offence, or alternatively, the Sentencing Council is advised to view identity theft as a significant aggravating factor in fraud cases.

7. – Numerous firms accept fraud as a business cost and inadequately prevent its facilitation. In June 2023, the UK Government outlined a new «failure to prevent fraud» offence aimed at promoting behavioural change and organisational accountability [65]. The new offence will make corporations liable if an employee commits a specified fraud offence for the organisation's gain and if the organisation lacks adequate fraud prevention measures. This offence applies to all large [66] corporations and partnerships across sectors, carrying the potential penalty of an unlimited fine.

a) HM Government 2023 Fraud Strategy

Fraud constitutes more than 40% of all crimes in the UK, yet police resources allocated to it are less than 1%. The goal of the three-year plan is to cut fraud by 10% from 2019 levels by the end of the current legislative session in 2025 [67]. The Strategy presents several commendable components yet given the substantial scale of fraud in the UK it might not suffice to turn the tide.

The Fraud Strategy is built upon three main pillars [68]:

(i) *Pursue Fraudsters*: Key initiatives include establishing a National Fraud Squad, implementing an intelligence-driven approach to disrupt fraudulent activities, substituting Action Fraud with a new state-of-the-art reporting system, increasing fraudsters' imprisonment, and leading global partnerships to remove obstacles to prosecute fraudsters worldwide. The first pillar lacks adequate resource allocation. Although the establishment of a National Fraud Squad staffed by 400 specialised investigators is promising,

[64] *Government Response to the Digital Identity and Attributes Consultation. Question 16*, 2023, https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/outcome/government-response-to-the-digital-identity-and-attributes-consultation.

[65] *Factsheet: Failure To Prevent Fraud Offence* (GOV.UK, 13 April 2023), https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/factsheet-failure-to-prevent-fraud-offence.

[66] The definition of large organisations is established in accordance with Companies Act 2006, which involves meeting at least two out of three criteria: 250+ employees, £36 million+ in turnover, and £18 million+ in total assets.

[67] HM Government (n 2).

[68] HM Government (n 2).

its operational details remain nebulous. At best, it might elevate the fraction of police dedicated to fraud from less than 1% to 1.5%.

(ii) *Block Fraudsters*: This pillar aims to significantly reduce the volume of fraudulent communications reaching the public. Measures include appointing an Anti-Fraud Champion [69], curbing criminals' misuse of the telephone network (banning cold calls on all financial products [70], banning SIM farms [71], reviewing the use of mass text aggregators and stopping more spoof calls), prompting the tech industry to actively prevent fraud through legislation and voluntary commitments, enhancing powers to shut down fraudulent websites, and sharing information about fraud prevalence on various platforms.

The industry-centric pillar introduces some sensible initiatives, like the prohibition of SIM farms (who needs them for any legitimate purpose?). However, the success of these measures hinges on the engagement of the tech sector.

(iii) *Empower the Public*: This aspect focuses on enabling individuals to effectively recognise, avoid, and report fraud. It encompasses providing support and reimbursement to more fraud victims and enhancing communication about fraud prevention and reporting [72].

The Strategy emphasises enhancing customer protection in financial institutions through measures like SCA, Confirmation of Payee (CoP), and the Banking Protocol. SCA requires authenticating customer identities during online transactions, mandated by Payment Services Regulations 2017 [73] – the same requirement adopted by all EU countries under PSD2.

CoP enables payers to confirm recipient account details, supported by an October 2022 PSR Policy Statement[74] directing 400 PSPs to expand CoP services. The EU recently put forth a similar provision, albeit with a delay

[69] A. BROWNE MP, https://www.gov.uk/government/people/anthony-browne.

[70] HM TREASURY, *Open Consultation: Ban on Cold Calling for Consumer Financial Services and Products*, (2023) https://www.gov.uk/government/consultations/ban-on-cold-calling-for-consumer-financial-services-and-products.

[71] HOME OFFICE, *Preventing the Use of SIM Farms for Fraud: Consultation* (2023) https://www.gov.uk/government/consultations/preventing-the-use-of-sim-farms-for-fraud/preventing-the-use-of-sim-farms-for-fraud-consultation-accessible.

[72] HM Government (n 2).

[73] The Payment Services Regulations 2017.

[74] *PSR, PS22/3 Extending Confirmation of Payee Coverage*, 2022; https://www.psr.org.uk/publications/policy-statements/ps22-3-extending-confirmation-of-payee-coverage/.

compared to the UK [75]. The Banking Protocol, led by UK Finance, equips banks to detect authorised fraud and collaborate with law enforcement [76]. Lastly, the Strategy outlines two pivotal initiatives: a risk-based approach for PSPs investigating potential fraudulent transactions and FCA evaluations of PSPs' fraud prevention systems.

8. – Currently, UK regulations mandate banks to reimburse victims of unauthorised fraud within 48 hours [77], but there is no equivalent provision for authorised fraud victims. In response to a super-complaint by Which? in 2016 [78], the PSR developed in 2019 the Voluntary Contingent Reimbursement Model (CRM) Code outlining conditions for reimbursing APP fraud victims [79]. Although ten PSPs have signed the CRM Code [80], reimbursement rates vary among them, and according to FOS 2020/2021 data, the Ombudsman ruled against banks in favour of customers in 73% of authorised fraud cases [81].

The UK Government addressed this issue by granting the PSR regulatory authority to mandate reimbursement from all PSR-regulated PSPs in relation to the Faster Payments System. In May 2022, the Treasury announced its intent to legislate [82], and in June 2023, the FSMA received

[75] EUROPEAN COMMISSION, *Revised Rules on Payment Services to Improve Consumer Protection and Competition in Electronic Payments*, 28 June 2023, https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544.

[76] *Expanding the Banking Protocol Scheme*, *UK Finance*, https://www.ukfinance.org.uk/news-and-insight/blogs/expanding-banking-protocol-scheme.

[77] This requirement mirrors the one imposed on all EU member states by PSD2.

[78] WHICH*? Super-Complaint Consumer Safeguards in the Market for Push Payments*, 2016, https://www.psr.org.uk/media/t0sln5vn/which-super-complaint-sep-2016.pdf.

[79] Lending Standards Board, *Written Evidence (FDF0050)*, 2022, https://committees.parliament.uk/writtenevidence/108066/html/.

[80] Current CRM Code signatories: Barclays Bank UK plc, The Co-Operative Bank plc, HSBC UK, Lloyds Banking Group, Metro Bank, Nationwide Building Society, NatWest Bank plc, Santander UK, Starling Bank, and Virgin Money UK.

[81] C. CAVAGLIERI, *Banks Wrongly Denying Fraud Victims Compensation in Up to 8 in 10 Cases*, in *Which?*, 11 November 2021. For instance, data from FOS 2020/2021 reveals that the Ombudsman overturned bank decisions in 86% of fraud cases involving RBS and NatWest.

[82] HM TREASURY, *Government Approach to APP Scam Reimbursement*, 2022, https://www.gov.uk/government/publications/government-approach-to-authorised-push-payment-scam-reimbursement/government-approach-to-authorised-push-payment-scam-reimbursement.

Royal Assent [83], allowing for this legislation to take effect. The focus on Faster Payments is due to its frequent use in APP fraud cases, accounting for 98% of such fraudulent payments in 2022 [84]. The UK's pioneering implementation of APP fraud reimbursement standards has garnered international attention from other jurisdictions [85]. The final PSR policy statement was issued in June 2023, and the new reimbursement requirement is scheduled to be implemented in 2024, with a specific date to be disclosed in Q4 2023 [86]. In the short to medium term, the policy is expected to result in an initial increase in reported APP fraud cases due to victim awareness and increased reporting by PSPs. However, a gradual decline in overall APP fraud incidents is anticipated over time.

The April deadline for implementation is much too soon given that the PSR has yet to establish final guidance and put in place an effective arbitration/dispute mechanism.

The novel reimbursement framework, backed by ten core policies, compels PSPs to promptly reimburse APP fraud victims within Faster Payments [87]. The reimbursement process mandates sending PSPs to compensate victims of APP fraud, with exceptions encompassing instances of first-party fraud or gross negligence, which is the customer standard of caution. Receiving PSPs are directed to share 50% of the reimbursement cost. The reimbursement window stands at 5 business days, with stop-the-clock provisions if needed. The 13-month claim timeframe mirrors PSD2 rules. Pending consultation, the claim excess and maximum reimbursement level are still to be finalised in Q4 2023. Importantly, the customer standard of caution and claim excess do not apply to vulnerable customers.

9. According to section 77(3) of the Payment Services Regulations 2017 [88] and as acknowledged in the CRM Code's exceptions to reimbursement, gross negligence is an established exception to PSP liability for unauthorised fraud. The FCA characterises gross negligence as follows: «*In line with the recitals to PSD2, we interpret gross negligence to be a higher standard than the standard of negligence under common law, demanding a high degree of carelessness*

[83] Financial Services and Markets Act 2023.

[84] UK Finance (n 54).

[85] Only two other markets, Japan and South Korea, have frameworks specific to APP fraud.

[86] PSR, *PS23/2 Fighting APP Fraud: A New Reimbursement Requirement. Response to September 2022 Consultation (CP22\4)*, (n 101).

[87] Excluded are civil disputes, payments via alternate systems, international transactions, and payments for unlawful purposes.

[88] The Payment Services Regulations 2017.

from customers» [89]. This exception places the burden of proof on the PSP, and it does not apply to vulnerable customers.

The interpretation of «gross negligence» is still evolving. The application of the reimbursement model and the rulings of disputed bank cases will shape the precise definition over time. Clarification is needed to guide consistent application. During the PSR September 2022 Consultation [90], the banking industry expressed concerns that gross negligence sets a demanding threshold for the customer standard of caution, potentially causing increased moral hazard by diminishing customer responsibility, heightened fraud due to decreased customer vigilance, and increased transactional friction. Consumer groups disagreed with these industry viewpoints. The PSR assessed gross negligence against alternative standards proposed by consultation participants but found no credible substitute [91]. In August 2023, the PSR introduced a consultation on the customer standard of caution outlining three customer care requirements: acknowledging PSP warnings, promptly reporting to the PSP, and responding to reasonable information requests by the PSP [92].

We do not believe that gross negligence should be used as the consumer caution exception. As stated in paragraph 4.19 of the consultation paper, the PSR recognises '*it can be hard to distinguish social engineering and sophisticated scam tactics from a lack of care by the consumer*'. In addition, it is very difficult to prove or disprove gross negligence in the context of payments, and so it should not be the only standard applied.

As previously mentioned, «vulnerable customers» are exempt from the application of the customer standard of caution and claim excess. The FCA has provided comprehensive guidance, endorsed by the PSR, to firms for the fair treatment of vulnerable customers [93]. This guidance entails firms recognising vulnerability characteristics within their target audience, setting

[89] FCA, *The FCA's Role Under the Payment Services Regulations 2017 and the Electronic Money Regulations* 2011, 2021, https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf.

[90] PSR, *CP22/4: APP Scams: Requiring Reimbursement*, 2022, https://www.psr.org.uk/publications/consultations/cp22-4-app-scams-requiring-reimbursement/.

[91] PSR, *PS23/2 Fighting APP Fraud: A New Reimbursement Requirement. Response to September 2022 Consultation (CP22\4)*, (n 101).

[92] PSR, *CP23/7: APP Fraud: The Consumer Standard of Caution*, 2023, https://www.psr.org.uk/publications/consultations/cp-23-7-app-fraud-the-consumer-standard-of-caution.

[93] FCA, *FG21/1 Guidance for Firms on the Fair Treatment of Vulnerable Customers*, 2021, https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf.

up supporting processes, and evaluating individual circumstances to ascertain if their vulnerability attributes, temporary or enduring, contributed to their fraud victimisation and thus meet the vulnerability criteria. According to the former Victims' Commissioner study, 22% of fraud victims exhibit high vulnerability [94] and approximately 700,000 individuals in the UK annually face severe vulnerability [95].

Banks are quite risk-averse about customer vulnerability, as disputes escalated to the FOS frequently lead to losses for them. Recognising that vulnerability is dynamic, varies across scenarios and evolves with fraud types, a one-size-fits-all approach cannot be adopted.

In the September 2022 Consultation, PSPs expressed concerns about heightened moral hazard due to the policy, but the evidence provided lacked quantitative support [96] and a PSR's lived experience workshop indicated that consumers anticipate minimal changes in their spending habits and payment practices due to the policy [97]. The Payments Association, representing 300+ firms, alerted the UK Government of '*unintended consequences*' of the policy. Firstly, they noted that the provision to refund all APP fraud victims might encourage fraud by people falsely presenting themselves as «vulnerable» to secure automatic reimbursement even in intentional cases. Secondly, the equal sharing of compensation costs between PSPs could prompt firms to be more cautious about opening accounts, disadvantaging low-income individuals («de-banking» effect) [98].

While we acknowledge that there certainly is the potential for customers to abuse the system by claiming certain transactions are fraudulent/scams when they are not, we actually hope that this new obligation will increase consumer awareness of APP scams and lead to a

[94] *Fraud Surged by 24% Under Covid. Now a New Study Reveals Around 700,000 Victims a Year Are Likely to Be Highly Vulnerable To Fraudulent Crime and Seriously Harmed By It*, (*Victims Commissioner*, 13 October 2021), https://victimscommissioner.org.uk/news/who-suffers-fraud/.

[95] S. POPPLETON, K. LYMPEROPOULOU, J. MOLINA, *Who Suffers Fraud? Understanding the Fraud Victim Landscape*, (Victims Commissioner 2021), https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/6/2021/12/VC-Who-Suffers-Fraud-Report-1.pdf.

[96] PSR, *CP22/4: APP Scams: Requiring Reimbursement*, (n 157).

[97] PSR, *PS23/2 Fighting APP Fraud: A New Reimbursement Requirement. Response to September 2022 Consultation (CP22\4)*, (n 101).

[98] PAYMENTS ASSOCIATION WARNS UK GOVT ON APP FRAUD PLANS, (*Finextra*, 27 June 2023) https://www.finextra.com/newsarticle/42555/payments-association-warns-uk-govt-on-app-fraud-plans.

more knowledgeable and wary customer base. Globally, regulators and industry experts are meticulously examining the UK's APP mandatory reimbursement protocols. As outlined below, Italian bank representatives' reactions to this measure express underlying concerns.

The UK «Make Banks Pay» approach is one possible solution, yet many actors involved in the fraud chain leverage interactions that do not exploit banks' vulnerabilities. As fraud continues to proliferate, regulatory pressure is expected to increase, but the issue of «economic responsibility» may fail to stop fraudsters. While reimbursement is crucial for securing justice for fraud victims, it should not be the sole focus of counter-fraud policy, as it is a 'downstream action that should be supported by upstream action' [99]**.** Blanket reimbursement may lead to moral hazard and increased fraud, with the mistaken perception that fraud is a 'victimless crime' [100]. Sharing responsibility is necessary, but expecting banks alone, as the final point in the fraud chain, to bear the entire fraud bill is unrealistic and this rationale was recently upheld in the case of *Philipp v Barclays Bank UK* [2023] UKSC 25 [101]. I hold a firm stance on this issue: implementing such a measure would likely amplify criminal activity and create risky moral hazard loopholes. The feasibility of this measure should be assessed on a country-specific basis, considering regional variations in criminal behaviour. This initiative appears somewhat populist in nature, driven by social unrest and economic turmoil, with the knee-jerk reaction being «compensation».

As already mentioned, when discussing the 2023 Fraud Strategy, to align responsibility and incentivise action, the Government should engage all fraud-enabling sectors, alongside the sending and receiving PSPs, in sharing the reimbursement costs [102]. According to UK Finance, '*a*

[99] PSR, *PS23/2 Fighting APP Fraud: A New Reimbursement Requirement. Response to September 2022 Consultation (CP22\4)*, (n 101).

[100] BUILDING SOCIETIES ASSOCIATION, *Written Evidence (FDF0023)* (2022) https://committees.parliament.uk/writtenevidence/108011/html/.

[101] *Philipp v Barclays Bank UK PLC [2023] UKSC 25.* This recent Supreme Court judgment focused on a bank's duty of care in APP fraud cases. The unanimous ruling confirmed the customer's authorisation of the transaction and highlighted the bank's obligation to swiftly carry out customer instructions without evaluating the wisdom or risks associated with their payment decisions. Although the impending introduction of mandatory APP fraud reimbursement may moderate the ruling's impact, it remains significant for potentially shaping the interpretation of customers' gross negligence. Even though the international transaction in question is not eligible for reimbursement, this case could set a precedent for similar fraud cases involving overseas payments.

[102] House of Lords (n 109).

reimbursement model alone will not slow the UK's growing epidemic of scams, nor prevent the non-financial impacts on customers and industry' [103].

While these reimbursement amounts might not harm banks, reimbursement shouldn't be granted for authorised transactions, as it would contradict PSD2 principles and undermine SCA. Alternatively, a model akin to MiFID could be adopted, requiring a similar form of «license» to be able to perform instant transfers. Instead, sharing reimbursement costs 50:50 between PSPs, holding receiving banks – frequently neobanks – partly liable, could promote accountability.

10. – In Italy, the domain of payment fraud is governed not only by the general provisions concerning the fulfilment of obligations and the «diligence required of mandatory» [104] and the bank in the «execution of instructions» [105] but also by the Italian Legislative Decree (D.lgs.) 11/2010 [106], issued in implementation of Directive PSD1 2007/64/EC [107], and subsequently amended by D.lgs. 218/2017 [108] in implementation of Directive "PSD2" 2015/2366/EU [109]. The offence of «computer fraud» is provided for in Article 640-ter of the Italian Penal Code [110], and in this context, one can also discuss the crimes of «identity theft»[111] and «unauthorised access to a computer or telematic system» [112]. Italy, like many other countries, does not categorise authorised fraud as a distinct form of fraud and its legislative and regulatory frameworks address fraud in a broader context.

a) Strong Customer Authentication (SCA)

In Italy, as of now, every payment transaction can only be carried out following the SCA requirement by PSPs, governed by Articles 97 and 98 of PSD2, as well as the Regulatory Technical Standards (RTS) on SCA issued by

[103] UK Finance, Response to Consultation CP22-4, December 2023.

[104] Article 1710, Italian Civil Code.

[105] Article 1856, Italian Civil Code.

[106] D.Lgs. 27 January 2010, No. 11.

[107] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market.

[108] D.Lgs. 15 December 2017, No. 218.

[109] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market.

[110] Defined as "any unauthorised alteration of a computer or telematic system, or the unauthorised intervention in any manner with data, information, or programs contained within a relevant computer or telematic system, with the intent of securing unjust profit for oneself or others to the detriment of another".

[111] Article 494, Italian Penal Code.

[112] Article 615-ter, Italian Penal Code.

the EBA and incorporated into the Regulation (EU) 2018/389 [113], amended by Regulation (EU) 2022/2360 [114]. The new Article 10-bis of the Italian D.lgs. 11/2010 [115], mandates that PSPs implement SCA when the user accesses their online payment account, initiates a payment transaction, and takes any action via a remote channel that may pose a risk of payment fraud. Moreover, in the case of online payment transactions, SCA must include elements linking the transactions to a specified amount and beneficiary through «dynamic linking» [116] by generating a unique authentication code (e.g. OTP [117]). SCA is a procedure based on the use of two out of three authentication factors: a «knowledge» factor (e.g., password), a «possession» factor possessed only by the user (e.g., smartphone, token), and an «inherence» factor inherent only to the user (e.g., fingerprint, facial recognition). Lastly, the concept of «independence» [118] is provided, ensuring that the breach of one of the aforementioned factors does not compromise the reliability of the others [119].

First and foremost, for a banking transaction to be valid, the consent of the consumer is essential as '*in the absence of consent, a payment transaction cannot be considered authorised*' [120]. In cases of unauthorised transactions by customers or incorrect execution by PSPs, customers are entitled to reimbursement of charged amounts and have a period of 13 months from the debit to request reimbursement [121]. Customers have several protection mechanisms to recover funds:

i) A refund request to the issuing intermediary;

[113] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017.

[114] Commission Delegated Regulation (EU) 2022/2360 of 3 August 2022.

[115] In accordance with Article 98, PSD2.

[116] Dynamic Linking is designed to intricately connect each transaction with its corresponding amount and the intended payment recipient. This overarching objective serves to thwart social engineering attacks, such as the notorious "man-in-the-middle" attack.

[117] One-Time Password.

[118] Article 9, Para. 1, Reg. (EU) 2018/389. See also ABF Milan Panel, Decs. n. 5895/2020 (https://www.arbitrobancariofinanziario.it/decisioni/2020/03/Dec-20200331-5895.PDF) and n. 1066/2019 (https://www.arbitrobancariofinanziario.it/decisioni/2019/01/Dec-20190116-1066.PDF).

[119] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017.

[120] Article 5, Para. 1, D.lgs. 11/2010.

[121] Article 9, D.lgs. 11/2010.

ii) Recourse to alternative dispute resolution systems (Banking and Financial Ombudsman – ABF[122]);

iii) Recourse to the Judicial Authority, which is the least frequently employed mechanism in this domain, due to its high costs, lengthy proceedings, and the need for exceptionally specialised expertise.

The user bears responsibility solely in cases of their own fraudulent actions or deliberate and severely negligent violation of duties pertaining to the safekeeping of payment instructions, authentication credentials, and prompt reporting of any irregularities (loss, theft, misappropriation, or unauthorised use of the payment instrument) [123]. The assessment of the client's fault has changed over time. In the initial rulings on the matter, clients were often considered concurrently at fault with the PSP due to negligent custody of access codes.[124] However, recently, a *favor* emerged towards the client that has been confirmed by the interpretation of the Italian Courts and the ABF. According to this interpretation, the PSP retains responsibility in all cases of unauthorised fraudulent transactions and a significant number of cases of authorised ones, as elaborated further below.

b) PSPs Liability and Burden of Proof

The burden of proof of the fraudulent, intentional, or grossly negligent behaviour by the customer, pursuant to Article 10, Paragraphs 1 and 2, D.lgs. 11/2010, falls upon the PSP [125]. In this regard, it is pertinent to refer to the significant decision of the ABF Coordinating Panel, Dec. n. 22745/2019 [126],

[122] The Banking and Financial Ombudsman (ABF) offers an extrajudicial alternative dispute resolution (ADR) to resolve disputes between customers and financial institutions, including banks, related to banking and financial transactions and services. For further information, consult https://www.arbitrobancariofinanziario.it/ and all the ABF Panels' decisions were consulted through the advanced research tool at https://www.arbitrobancariofinanziario.it/decisioni/index.html.

[123] Article 7, D.lgs. 11/2010.

[124] C. VALENTINI, *Phishing: il cliente della banca vince facile*, *Bancaria*, 345, 2022.

[125] ABF Coordinating Panel, Dec. 897/2014 (https://www.arbitrobancariofinanziario.it/decisioni/2014/02/Dec-20140214-897.pdf) and Cassazione Civile, Sect. VI, 12/04/2018 Dec. No. 9158.

[126] ABF Coordinating Panel, Dec. No. 22745/2019, pag. 7, para. 8: "*Si osserva che l'onere probatorio previsto nei commi 1 e 2 dell'art. 10 del decreto deve necessariamente essere assolto dal PSP con riguardo ad ambedue i profili (autenticazione ed esecuzione delle operazioni di pagamento, nonché colpa grave dell'utilizzatore), da ritenersi necessari e*

which states that the evidentiary burden must necessarily be fulfilled by the PSP with respect to both aspects: (i) proper authentication, recording, accounting, and execution of payment transactions, as well as (ii) proof of fraud, intent, or gross negligence by the user. These two proofs are deemed necessary and complementary [127]. Moreover, as stated by the ABF Coordinating Panel, the proof must be provided by the PSP through "*clear, precise, and consistent indications*" [128]. Furthermore, as highlighted by the ABF Naples and Milan Panels, the evaluation of the customer's conduct must be based on the consideration "*of the set of circumstances that characterise the specific case*" [129]. The burden of proof incumbent upon the PSP must also be read in conjunction with the general principle established by Article 1218 of the Italian Civil Code [130], which – based on the interpretation of the Italian Supreme Court of Cassation [131] and embraced by various ABF Panels [132] –

complementari." (https://www.arbitrobancariofinanziario.it/decisioni/2019/10/Dec-20191010-22745.PDF).

[127] This orientation is also supported by Cassazione Civile Dec. n. 9158/2018 and Milan Court of Appeal, Sect. I, 23/07/2021 Dec. n. 2419.

[128] ABF Coordinating Panel, Dec. n. 897/2014, pag. 7: "*Ma vi è di più: l'intermediario ha addotto una serie di indizi chiari, precisi e concordanti idonei a comprovare che l'operazione disconosciuta è stata posta in essere mediante l'impiego della carta e del codice dispositivo […]*" (https://www.arbitrobancariofinanziario.it/decisioni/2014/02/Dec-20140214-897.pdf).

[129] ABF Milan Panel, Dec. No. 2594/2012, pag. 3: "*Occorre infatti collocare tale evento nelle circostanze del singolo caso al fine di valutare se esso sia sufficiente a dimostrare che la indebita autorizzazione conferita mediante l'uso di tali codici sia frutto o meno di una colpa grave del cliente.*" (https://www.arbitrobancariofinanziario.it/decisioni/2012/07/Dec-20120725-2594.pdf) and ABF Naples Panel 1802/2013, pag. 4: "*Alla luce del complesso delle circostanze sopra delineate, questo Collegio ritiene soddisfatto l'onere di dimostrare, da parte dell'intermediario, la grave negligenza della titolare della carta, al fine di liberarsi dalla presunzione di responsabilità derivante dall'utilizzo non autorizzato della carta di debito.*" (https://www.arbitrobancariofinanziario.it/decisioni/2013/04/Dec-20130403-1802.pdf).

[130] «Liability of debtor».

[131] Cassazione Civile, Sect. I, 24 settembre 2009, Dec. n. 20543 ("*La diligenza del buon banchiere deve essere qualificata dal maggior grado di prudenza e attenzione che la connotazione professionale dell'agente consente e richiede. Tale diligenza trova applicazione non solo con riguardo all'attività di esecuzione di contratti bancari in senso stretto, ma anche in relazione ad ogni tipo di atto od operazione che sia oggettivamente esplicato presso una struttura bancaria e soggettivamente svolto da un funzionario bancario. Inoltre la diligenza di cui trattasi va valutata, non in base a criteri rigidi e predeterminati, ma considerando le cautele e gli accorgimenti che le circostanze del caso concreto suggeriscono.*") and Cassazione Civile, Sect. I, 12 gugno 2007 Dec. n. 13777 ("*In materia di rapporti bancari*

requires the PSP to prove that it has fulfilled the obligations of custody and safeguarding of client funds with «qualified diligence» [133], namely the diligence of a *bonus nummarius* (prudent banker)[134], considering also that in contractual relationships with the customer, "*the bank is answerable according to the rules concerning mandate*"[135].

If the PSP fails to meet the evidentiary burden, it is obligated, as stipulated by Article 11 of D.lgs. 11/2010, to promptly recredit the amount deducted from the customer's current account upon registering the fraudulent transaction within the close of the next operational day following the occurrence. This provision aims to restore the account "*to the state it would have been in if the payment transaction had not taken place*". However, in cases of reasonable suspicion of fraud, the PSP has the authority to suspend reimbursement to investigate the matter, informing the Italian Central Bank through immediate written communication. With a few borderline cases aside, the bank holds substantial proof to differentiate between fraud and a scam scenario. It looks at factors like transaction location, history, and device used. The bank's verification process is crucial in determining reimbursement eligibility, differentiating between fraud (eligible) and scams (not eligible).

---

va precisato che la banca è tenuta ad adempiere tutte le obbligazioni assunte nei confronti dei propri clienti con la diligenza particolarmente qualificata dell'accorto banchiere, non solo in relazione all'attività di esecuzione di contratti bancari in senso stretto, ma anche con riferimento ad ogni tipo di atto o di operazione oggettivamente esplicati. Pertanto, la banca emittente della carta bancomat è responsabile, fino a prova contraria, della predisposizione dei mezzi meccanici, della loro idoneità e del loro funzionamento e, comunque, degli errori dovuti a dolo o colpa grave.").

[132] ABF Rome Panel, Dec. 960/2012, (https://www.arbitrobancariofinanziario.it/decisioni/2012/03/Dec-20120330-960.pdf), ABF Naples Panel, Decs. n. 2191/2012 (https://www.arbitrobancariofinanziario.it/decisioni/2012/06/Dec-20120627-2191.pdf), and n. 1725/2012 (https://www.arbitrobancariofinanziario.it/decisioni/2012/05/Dec-20120528-1725.pdf).

[133] Article 1176, Par. 2, Italian Civil Code ("Diligence in performance").

[134] In line with ABF Bari Panel, Dec. n. 13094/2017 (https://www.arbitrobancariofinanziario.it/decisioni/2017/10/Dec-20171020-13094.PDF), which follows Cassazione Civile, Sect. I., 3 febbraio 2017 Dec. n. 2950. According to the Cassazione, "*the diligence required of the professional has a technical nature and must be evaluated considering the typical risks of the relevant professional sphere, thus taking as a benchmark the prudent banker*" (in line with Cassazione, Dec. n. 13777/2007).

[135] Article 1856 Italian Civil Code.

11. – Regarding recent EU efforts to combat payment fraud, there are key initiatives: Directive (EU) 2019/713 addressing fraud and counterfeiting of non-cash payments [136], Regulation (EU) 'DORA' 2022/2554 focusing on Digital Operational Resilience for the Financial Sector [137], and a legislative proposal for a regulation on instant payments published on 26 October 2022 [138]. Furthermore, the European Commission (EC) evaluated PSD2 in 2022 and released revised rules on June 28, 2023, aimed at enhancing consumer protection and fostering competition in electronic payments [139].

In these revised rules, the EC prioritises combatting payment fraud and emphasises that modifications to the PSD2 liability structure must diminish fraud while avoiding moral hazard. Evolving fraud types, which blur the line between unauthorised and authorised transactions, exceed the scope of PSD2, emphasising the necessity for the introduction of PSD3.

Consequently, the Commission suggested proactive anti-fraud measures:

(i) Extending IBAN/name-matching verification services to all credit transfers for euro instant payments in the EU, offered free to consumers;
(ii) Establishing a legal basis for PSPs to share fraud-related information without violating GDPR via dedicated IT platforms;
(iii) Strengthening transaction monitoring;
(iv) Requiring PSPs to enhance customer and staff fraud awareness;
(v) Expanding consumer refund rights in specific circumstances;
(vi) Imposing obligations on telecom operators to collaborate with PSPs in preventing fraudulent activities and scams [140].

The proposal introduces refund rights in two scenarios: for consumers affected by the IBAN/name verification service's failure to detect a mismatch, and for those deceived by «spoofing» fraud, where fraudsters impersonate the consumer's bank employees. Victims of spoofing fraud may seek damages from their PSP under specific conditions, requiring a police report and prompt notification, and refunds would not be permitted in cases of victim «gross negligence». This proposal is similar to the new UK PSR's

[136] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019.

[137] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022.

[138] Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) No 260/2012 and (EU) 2021/1230.

[139] European Commission (n 138).

[140] Ibid.

APP reimbursement requirement, albeit narrower in scope, focusing solely on impersonation fraud rather than covering all APP fraud [141].

Finally, there are proposals to enhance the existing SCA framework, including clarifying when certain transactions can be exempt from SCA while still safeguarding against fraud, simplifying SCA application for payment account information services, strengthening the use of digital passthrough wallets by mandating SCA during payment instrument enrolment under PSP responsibility, and ensuring diverse SCA methods accessible to all users, accommodating various needs and situations without reliance on a single technology or device, such as a smartphone [142].

12. – Payment fraud, a global «epidemic» [143], exhibits a dynamic nature and is perpetrated with ever-adapting tactics. Despite being a regulated operational risk, there remains a significant '*dark figure of undetected and detected but unreported and unrecorded*'[144] fraud incidents, stemming from the tendency to downplay its severity. This has resulted in an accountability gap within the fragmented realm of stakeholders tasked with addressing this issue. This work explored three core research areas, informed by expert interviews: payment fraud evolution in digital banking, the efficacy of legislative tools in the UK and Italy against modern payment fraud, and countermeasures for both legal systems. A thorough analysis of payment fraud laws in the UK and Italy uncovers remarkable similarities in policy outcomes. The UK's proactive approach could serve as a "crystal ball", a predictive model, for countries like Italy, offering insights into future fraud trends and preventive strategies. Despite the UK mandating APP fraud reimbursement from 2024, and Italy requiring reimbursement solely for unauthorised fraud cases, both countries adopt customer-centric systems, placing the burden of proof on the PSPs through a strict liability approach, akin to a *probatio diabolica*. Both the UK's FOS and Italy's ABF have been gradually shifting their rulings in favour of the customers, even in cases involving authorised fraud. The ongoing debate surrounding fraud reimbursement calls for comprehensive, multi-sectoral solutions that avoid

[141] Refer to the EC's legislative proposal on Instant Payments published on October 26, 2022.

[142] S. ELLENA, *EU Commission Updates Payment Rules to Fight Fraud, Improve Consumer Rights*, (*www.euractiv.com*, 28 June 2023).

[143] K. WESTMORE, J. HOLMES, *The Fraud Epidemic* (*RUSI*, 18 March 2022), https://rusi.org/podcasts/suspicious-transaction-report/episode-6-fraud-epidemic.

[144] M. LEVI, M. SMITH, *Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19*, Research report n. 19 Canberra, https://doi.org/10.52922/rr78115.

exacerbating customer moral hazard while holding all fraud-enabling sectors accountable.

Addressing payment fraud requires a concerted effort from both the public and private sectors, but it is challenging due to the scarcity of reliable data, a lack of consensus on effective solutions, its global reach, and its ever-evolving nature driven by dynamic perpetrators and vulnerabilities. Governments should adopt a risk-based approach to payment fraud, emphasizing ongoing assessment and implementation of adaptive mitigations, rather than seeking a one-size-fits-all solution. This dissertation outlines five domains of countermeasures, applicable to Italy, the UK, and similar legislative contexts: legislation, law enforcement, data sharing, customer empowerment through awareness and victim support, and the utilisation of Industry 4.0 technologies. While legislative reforms and enhanced law enforcement are vital, effectively combating payment fraud necessitates engaging in complex discussions regarding incentives and disincentives within all fraud-enabling sectors, with a particular focus on social media platforms and telecom companies, to recalibrate their share of accountability within the fraud bill.

Abstract

PAYMENT FRAUD IN ITALY AND THE UK: COMPARATIVE ANALYSIS AND PROSPECTS FOR REFORM

Questo lavoro indaga gli aspetti chiave delle frodi nei pagamenti bancari digitali in Italia e nel Regno Unito (UK), sfruttando anche le informazioni ricavate dalle interviste agli esperti del mondo bancario. In primo luogo, esplora la natura in evoluzione delle frodi nei pagamenti, evidenziando il loro passaggio da forme non autorizzate a forme autorizzate. In secondo luogo, valuta l'efficacia degli strumenti legislativi esistenti in Italia e nel Regno Unito, sottolineando la loro dipendenza dai processi politici. Da ultimo, analizza anche la proposta di direttiva PSD3 mettendone in luce aspetti positivi e criticità.

This work investigates the key aspects of digital banking payment fraud in Italy and the United Kingdom (UK), also exploiting the information obtained from interviews with experts in the banking world. First, it explores the evolving nature of payment fraud, highlighting its shift from unauthorized to authorized forms. Secondly, it evaluates the effectiveness of existing legislative instruments in Italy and the United Kingdom, highlighting their dependence on political processes. Finally, it also analyzes the proposed PSD3 directive, highlighting its positive aspects and critical issues.
